REINERSCT

mate*Suite*

Installations- und Bedienungsanleitung

Die clevere Sicherheits-Software
für PC und Chipkartenleser

Inhaltsverzeichnis

Kapitel 1 Was ist neu in Version 2.0 3

Kapitel 2 Einführung in mateSuite 3

Kapitel 3 Versions-/ Lizenzinformationen 4

Kapitel 4 Systemvoraussetzungen 5

Kapitel 5 Die Software 5

5.1 mateSuite - Einrichtungsassistent ... 5

Schritt 1 - Einrichtung Chipkartenleser ... 6
Schritt 2 - Systemvorbereitung ... 6
Schritt 3 - Erfassen von Chipkarten ... 7
Schritt 4 - Einrichtung loginMate ... 9
Schritt 5 - Einrichtung passMate ... 12
Schritt 6 - Einrichtung cryptMate ... 16

5.2 mateSuite-Administrator ... 20

mateSuite-Anwendungen ... 21
loginMate ... 22
Konten erstellen ... 23
Kontenverwaltung ... 25
Kontenbeschränkung/Erweiterte Anmeldung ... 27
Anmelden/Abmelden/Sperren/Entsperren ... 29
Anmeldung ... 29
Benutzerkonto wählen ... 31
Sperren ... 31
Runterfahren ... 34
Funktion STRG+ALT+ENTF ... 34
Einstellungen ... 36
passMate ... 37
Passworteinträge manuell anlegen ... 38
Pasworteinträge bearbeiten ... 41
Internet Explorer-Plugin ... 42
passMate-Manager ... 45
Einstellungen ... 47
cryptMate ... 48
Virtuelles Laufwerk erstellen und verschlüsseln ... 49
Verwaltung von virtuellen Laufwerken ... 51
cryptMate-Manager ... 54
Einstellungen ... 55
Verschlüsseln von Dateien und Ordner ... 56
smartMate ... 60
SmartCard Informationen einsehen ... 60
GSM Snap In ... 61
Einträge bearbeiten/erstellen ... 62
Import/ Export ... 63
Nummern internationalisieren ... 65
TAN-Generator ... 66
Verwaltung ... 67
mateSuite Suspend Manager ... 70
mateSuite AutoSuspend ... 71
Berechtigungen ... 73

Kapitel 6 Unterstützte Chipkarten 76

6.1 mateKey Security Card 76

Kapitel 7 Unterstützte Chipkartenleser 78

Kapitel 8 Anregungen/Support/Updates 78

Kapitel 9 mateSuite-Glossar 79

Index 80

1 Was ist neu in Version 2.0

Gegenüber der Version 1.3 wurde die mate***Suite*** in der Version 2.0 stark verbessert. Neben vielen kleineren Erweiterungen und Korrekturen wurden folgende Features integriert:

- Unterstützung Microsoft Vista 32 Bit
- Ab Vorabversion **V2.0.10** Unterstützung Windows 7 32/64 Bit
- Neues Design - Optimiert für den Windows XP-Stil
- Neuer cryptMate Laufwerksassistent
- Netzwerk-Freigabe nun möglich
- Erweiterte Laufwerksoptionen bei cryptMate
- Völlig überarbeitete GSM Unterstützung in smartMate
- Anwenderdaten (passMate DB, cryptMate Laufwerke, loginMate DB) nun in den von Microsoft vorgesehenen Benutzerverzeichnissen

2 Einführung in mateSuite

mate***Suite*** integriert verschiedene Sicherheitsanwendungen für Chipkarten und Chipkartenleser. Mit Hilfe von mate***Suite*** können Sie Ihre Chipkarte multifunktional nutzen: Vom Auslesen der Karte, über das sichere Verwalten von Passwörtern, bis hin zur Verschlüsselung von Laufwerken, bietet mate ***Suite*** ein breites Spektrum an Datenschutz- und Sicherheitsfunktionalität für Ihre Rechnerumgebung.

login***Mate***®	**Login mit Chipkarten für Windows /XP 32 Bit/2003 Server/ Vista 32Bit** Mit login***Mate***® können Sie Ihren Windows 2003 Server-/XP-/ Vista-PC mittels Chipkartentechnologie absichern. Hierfür übernimmt login***Mate***® die Steuerung der Windows-Anmeldung. Anstatt einer Passworteingabe, wird der PC mit einer Chipkarte freigeschaltet.
crypt***Mate***®	**Speicherung vertraulicher und sensibler Daten auf speziell verschlüsselten virtuellen Laufwerken** Mit crypt***Mate***® können auf Datenträgern (Festplatten, USB-Sticks, Internet-Laufwerken etc.) virtuelle verschlüsselte Laufwerke eingerichtet werden. Diese Laufwerke werden mittels Chipkarte verschlüsselt. Das Laufwerk wird erst freigeschaltet, wenn die entsprechende Karte in den Chipkartenleser eingeführt wird.
pass***Mate***®	**Verwaltung beliebiger PC- und Internet-Zugangsberechtigungen** pass***Mate***® erleichtert die Verwaltung von Passwörtern und gewährleistet dabei eine hohe Sicherheit. Die sensiblen Passwortdaten werden in einer verschlüsselten Datei oder direkt auf der mateKey Security Card abgespeichert. Aus dieser Datenbank können Sie dann automatisch in die gewünschte Applikation oder der Eingabemaske des Browsers eingefügt werden.
smart***Mate***®	**Anzeigen und Bearbeiten von Daten verschiedener Chipkarten** Mit smart***Mate***® lassen sich Informationen zu den von mate ***Suite*** unterstützten Chipkarten auslesen. Je nach Kartentyp sind der Umgang der Informationen und die Bearbeitungsmöglichkeiten sehr unterschiedlich. Alle Informationen lassen sich auch ausdrucken.

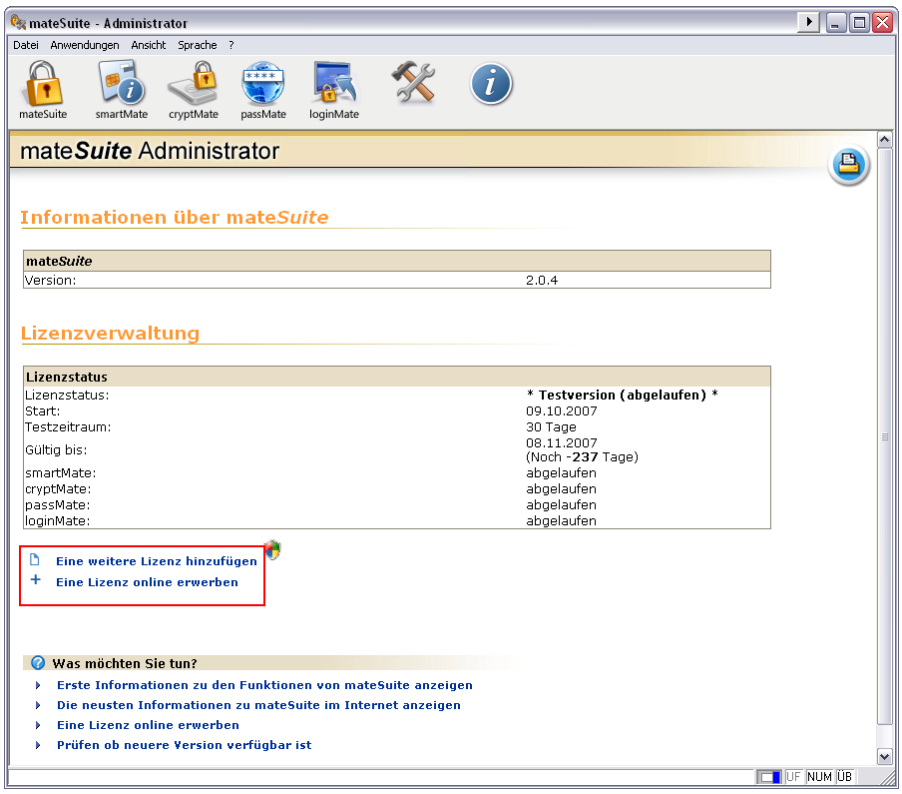
Alle Anwendungen können bequem über den mateSuite-Administrator verwaltet werden.

Die Installation der Software und die weiterführenden Schritte sollten von einen Administrator oder jemanden der administrative Rechte hat ausgeführt werden.

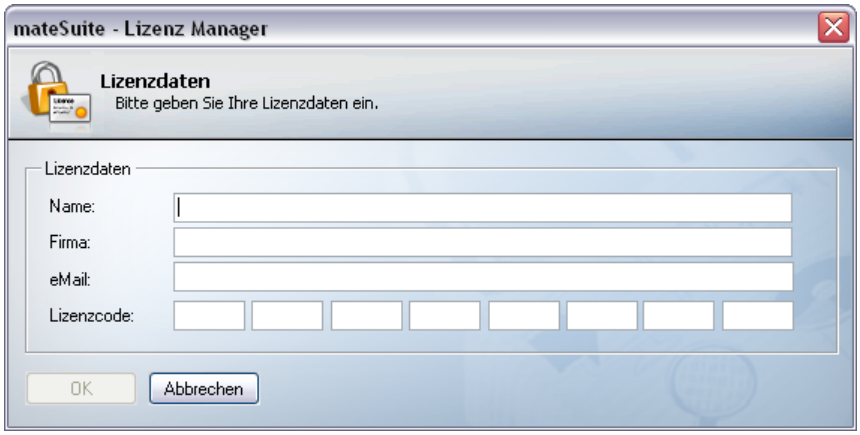
Überall, wo dieses Symbol steht, werden die Einstellung systemweit vorgenommen und erfordern somit administrative Rechte.

3 Versions-/ Lizenzinformationen

Über die Infoseite lässt sich die installierte Version und der Umfang der mateSuite-Lizenzierung ermitteln.



Sie haben die Möglichkeit weitere Anwendungen käuflich zu erwerben und hier zu lizenzieren.



4 Systemvoraussetzungen

- IBM – kompatibler PC mit mindestens 256 MB Arbeitsspeicher (empfohlen 512 MB)
- 100 MB freien Festplattenspeicher
- Grafikkarte: mindestens 1024x768 / 256 Farben (besser 32.000)
- CD ROM Laufwerk
- Serielle/ USB Schnittstelle zum Anschluss des Lesegerätes
- XP 32 Bit/ 2003 Server/Vista 32 Bit
- Internet Explorer 6.0

Ab der Vorabversion V2.0.10 ist die Software mate***Suite*** Windows 7 32/64 Bit kompatibel.

5 Die Software

Die mateSuite Software besteht aus zwei Programmteilen. Im Einrichtungsassistenten, der gleich nach der Installation startet, können Sie die ersten Einrichtungen vornehmen. Im mateSuite Administrator können Sie weiterführende Einstellungen der einzelnen Programmteile vornehmen.

5.1 mateSuite - Einrichtungsassistent

Der mate***Suite***-Einrichtungsassistent wird im Rahmen der mate***Suite***-Installation aufgerufen. Hier können alle mate***Suite***-Anwendungen konfiguriert werden.

Die Vorgehensweise zur Einrichtung ist bei allen Anwendungen identisch:

Zuerst wird das mate***Suite***-Objekt (passMate-Datenbank, cryptMate-Laufwerk, loginMate-Konto) angelegt und dessen Eigenschaften festgelegt. Anschließend werden die Berechtigung zum Zugriff auf diese mate***Suite***-Objekte definiert. Als Berechtigungen dienen die erfassten Chipkarten.

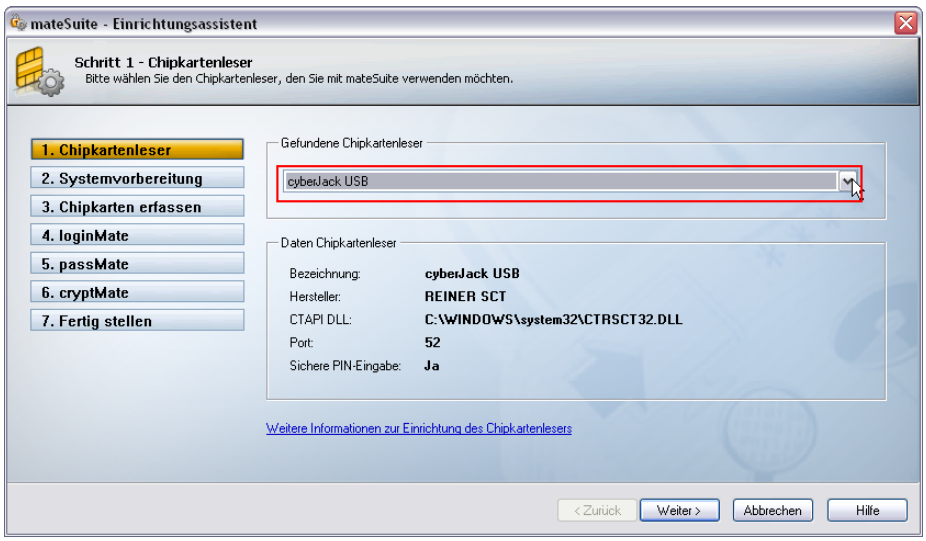
Über den Menüpunkt **? > Einrichtungsassistent** im mateSuite-Administrator oder im Programmpfad **Start > Programme > REINER SCT mateSuite > Einrichtungsassistent** kann der Assistent jederzeit erneut gestartet werden.

Folgende Schritte werden beim Ausführen des Einrichtungsassistenten der Reihe nach vollzogen.

- Schritt 1 - Einrichtung Chipkartenleser
- Schritt 2 - Systemvorbereitung
- Schritt 3 - Erfassen von Chipkarten/Schlüsseln
- Schritt 4 - Einrichtung loginMate
- Schritt 5 - Einrichtung passMate
- Schritt 6 - Einrichtung cryptMate

5.1.1 Schritt 1 - Einrichtung Chipkartenleser

Bei der erstmaligen Installation von mate***Suite*** sucht das Programm automatisch nach bereits installierten Chipkartenlesern und führt diese in einer Auswahlliste auf. Wählen Sie aus der Liste das Gerät aus, welches standardmäßig mit mate***Suite*** verwendet werden soll.



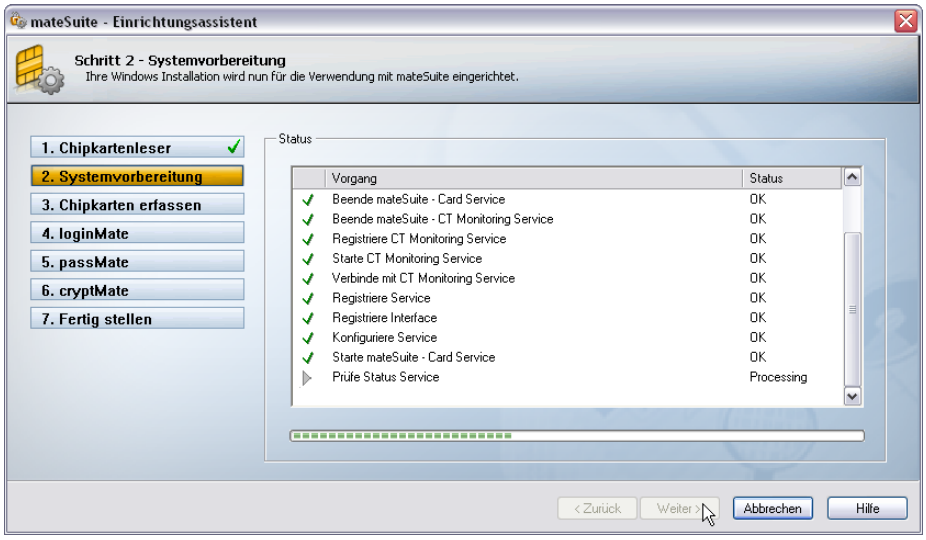
Klicken Sie auf den Button **Weiter** und es folgt Schritt 2.

Weitere Informationen

- Unterstützte Chipkartenleser

5.1.2 Schritt 2 - Systemvorbereitung

Bevor mate***Suite*** konfiguriert werden kann, überprüft der Einrichtungsassistent, ob alle notwendigen Dienste vorhanden und gestartet sind. Gegebenenfalls werden auch Reparaturen am System durchgeführt.

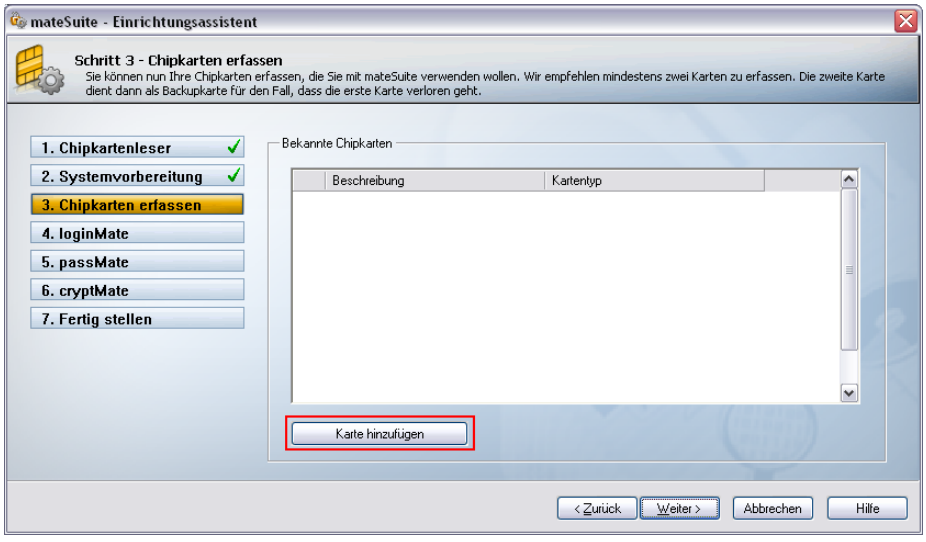


Nach bestandener Prüfung folgt der Schritt 3.

5.1.3 Schritt 3 - Erfassen von Chipkarten

mate***Suite*** verwendet die auf Chipkarten enthaltenen kryptographischen Schlüssel, um mateSuite-Objekte (passMate-Datenbanken, cryptMate-Laufwerke, loginMate-Konten) zu verschlüsseln und zu sichern.

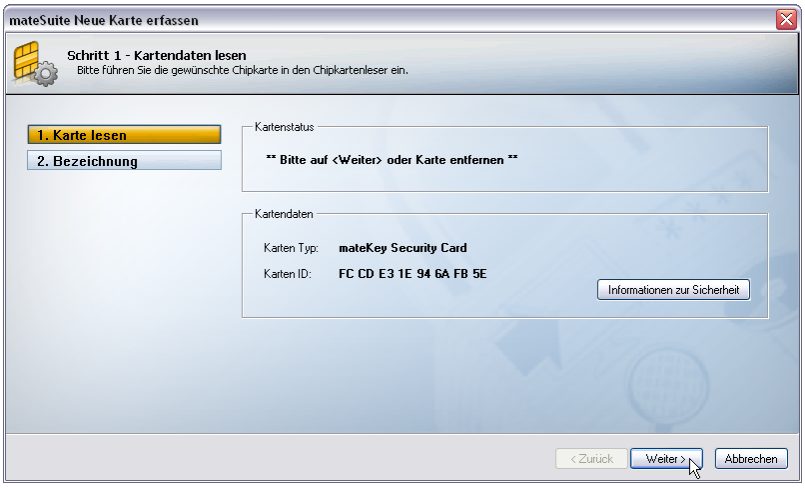
Bei der Neuinstallation von mate***Suite*** müssen deshalb zunächst eine oder mehrere Chipkarten erfasst werden.


mateSuite - Einrichtungsassistent
Schritt 3 - Chipkarten erfassen
Sie können nun Ihre Chipkarten erfassen, die Sie mit mateSuite verwenden wollen. Wir empfehlen mindestens zwei Karten zu erfassen. Die zweite Karte dient dann als Backupkarte für den Fall, dass die erste Karte verloren geht.
1. Chipkartenleser
2. Systemvorbereitung
3. Chipkarten erfassen
4. loginMate
5. passMate
6. cryptMate
7. Fertig stellen
Bekannte Chipkarten
Beschreibung
Kartentyp
Karte hinzufügen
< Zurück
Weiter >
Abbrechen
Hilfe

Um Chipkarten in mate***Suite*** zu integrieren, gibt es einen Assistenten, mit dem in zwei Schritten Chipkarten als Berechtigungen in mate***Suite*** eingelesen werden. Dazu wird die Chipkarte in den Leser eingesteckt. Drücken Sie den Button **Karte hinzufügen** und der Assistent startet.

Schritt 1 - Kartendaten lesen

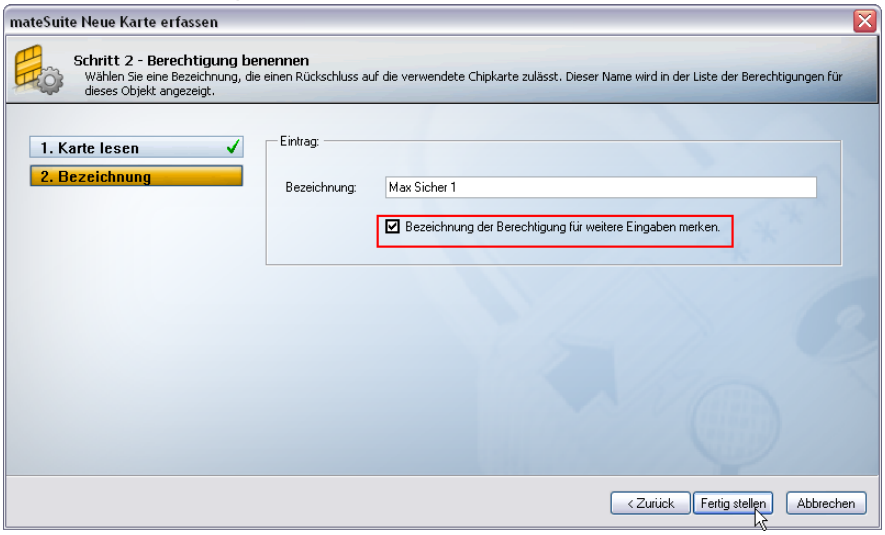
mate***Suite*** analysiert die Karte und stellt den Kartentyp fest und ob die Karte zur Verwendung geeignet ist.


mateSuite Neue Karte erfassen
Schritt 1 - Kartendaten lesen
Bitte führen Sie die gewünschte Chipkarte in den Chipkartenleser ein.
1. Karte lesen
2. Bezeichnung
Kartenstatus
** Bitte auf <Weiter> oder Karte entfernen **
Kartendaten
Karten Typ: mateKey Security Card
Karten ID: FC CD E3 1E 94 6A FB 5E
Informationen zur Sicherheit
< Zurück
Weiter >
Abbrechen

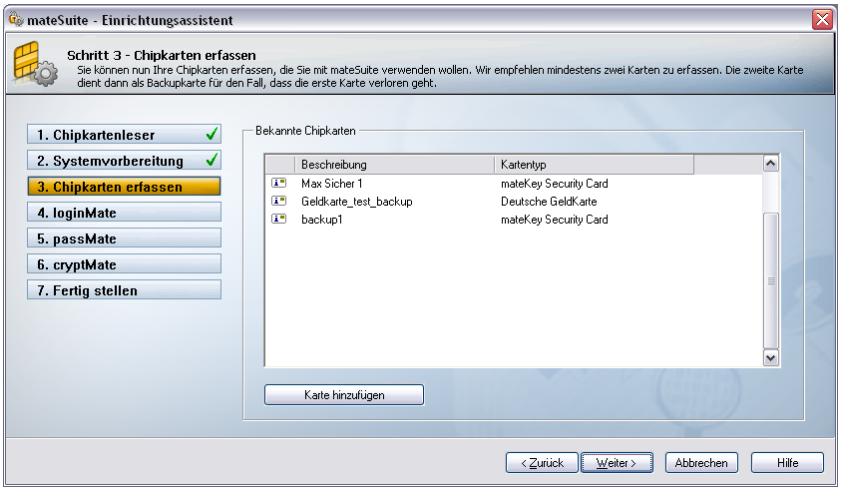
Bei PIN-geschützten Chipkarten ist an dieser Stelle die Eingabe der PIN erforderlich!

Klicken Sie auf den Button **Weiter** und es folgt Schritt 2.

Schritt 2 - Eintrag benennen


mateSuite Neue Karte erfassen
Schritt 2 - Berechtigung benennen
Wählen Sie eine Bezeichnung, die einen Rückschluss auf die verwendete Chipkarte zulässt. Dieser Name wird in der Liste der Berechtigungen für dieses Objekt angezeigt.
1. Karte lesen
2. Bezeichnung
Eintrag:
Bezeichnung:
Max Sicher 1
Bezeichnung der Berechtigung für weitere Eingaben merken.
< Zurück
Fertig stellen
Abbrechen

Durch Aktivierung der Option *Merke den Schlüsselnamen für weitere Eingaben* wird bei späterem Einstecken der Karte immer genau der vorgegebene Name angezeigt.
Klicken Sie auf **Fertig stellen** und die eingerichteten Chipkarten/Berechtigungen werden nun angezeigt.



Es wird dringend empfohlen, zur Verschlüsselung von mate*Suite*-Objekten immer mindestens zwei Chipkarten zu verwenden, da auch REINER SCT nicht in der Lage ist, verschlüsselte Dateien wiederherzustellen, sollte die einzige verwendete Karte defekt sein oder verloren gehen.

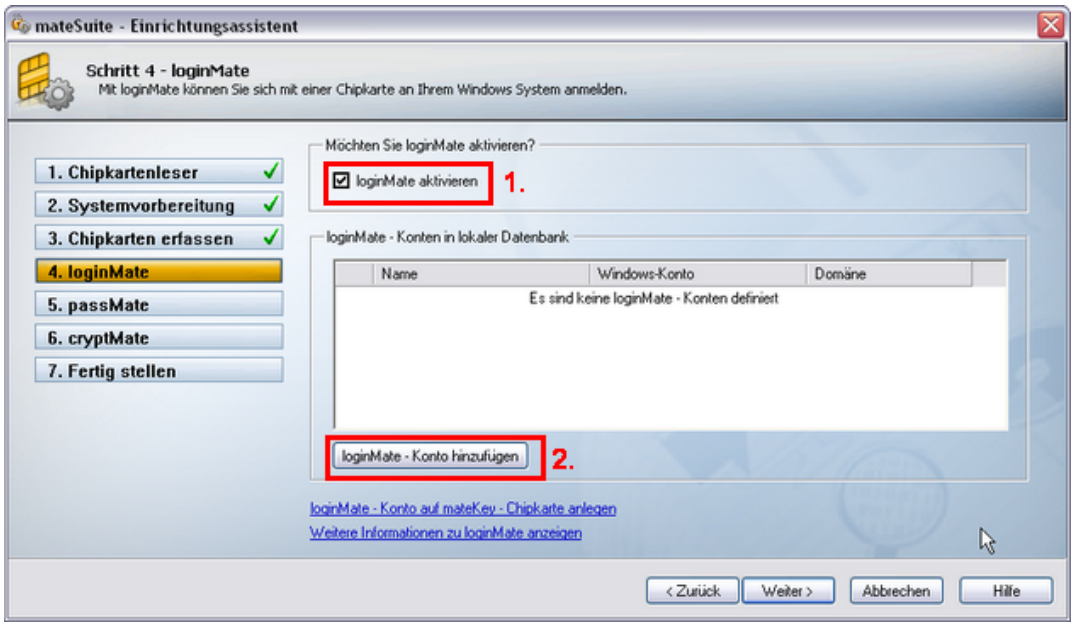
Verschiedene Hersteller von Signaturkarten sind in der Lage, bei Verlust wieder eine Karte mit identischen Schlüsseln herzustellen. Info's erhalten Sie über den Lieferanten der eingesetzten Karte.

Weitere Informationen:

▸ Verwaltung Bekannte Karten.

5.1.4 Schritt 4 - Einrichtung loginMate

In diesem Schritt richten Sie login***Mate***®-Konten ein.



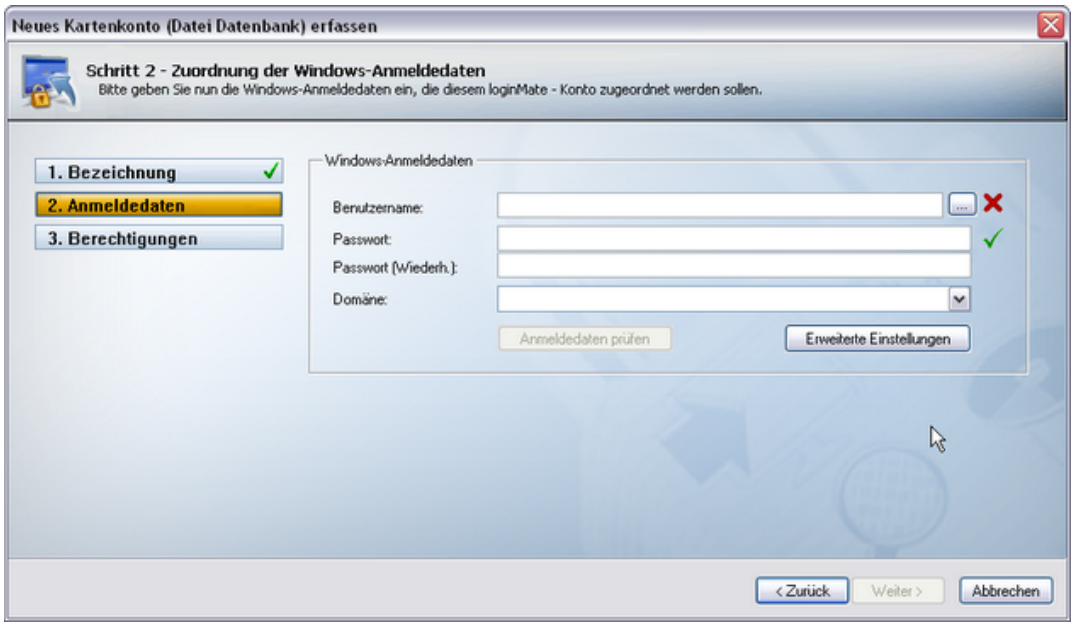
1. Aktivieren Sie loginMate
2. Hinzufügen eines neuen loginMate Kontos

Hinzufügen eines loginMate Kontos

1. Bezeichnung

Vergeben Sie einen Namen des neuen Kontos.

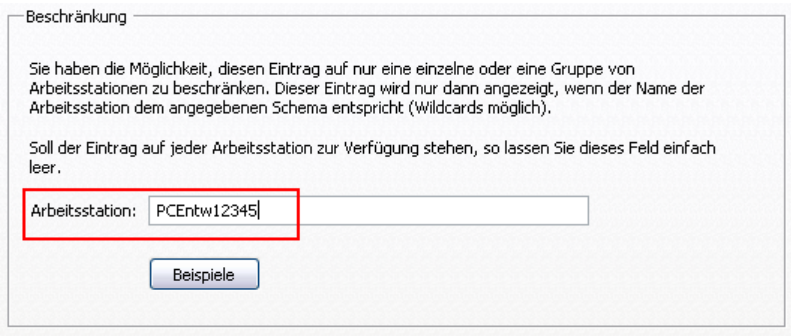
2. Anmeldedaten



Geben Sie hier einen Benutzernamen, ein Passwort und die Domäne eines vorhandenen Windows-Accounts an. Mit **Anmeldedaten prüfen** können Sie schauen, ob die Daten korrekt angelegt sind.

- **Erweiterte Einstellungen:**
  Hier können Sie weiterführende Einstellungen vornehmen. Bei **Beschränkung** können Sie anhand des Computernamens Ihre login***Mate***® Konten verschiedenen Rechnern zuordnen. Hierzu weisen Sie den einzelnen Konten Beschränkungen zu. Sie können diese Beschränkungen bereits bestehenden Konten oder neuen Konten zuweisen.

  - **Beispiel:**
    Sie haben einen PC mit dem Computernamen **PCEntw12345**. Jetzt soll der Mitarbeiter sich nur an diesem Computer anmelden dürfen. Dazu tragen Sie den Computernamen der Arbeitsstation bei Beschränkungen ein.


Beschränkung
Sie haben die Möglichkeit, diesen Eintrag auf nur eine einzelne oder eine Gruppe von Arbeitsstationen zu beschränken. Dieser Eintrag wird nur dann angezeigt, wenn der Name der Arbeitsstation dem angegebenen Schema entspricht (Wildcards möglich).
Soll der Eintrag auf jeder Arbeitsstation zur Verfügung stehen, so lassen Sie dieses Feld einfach leer.
Arbeitsstation:
PCEntw12345
Beispiele

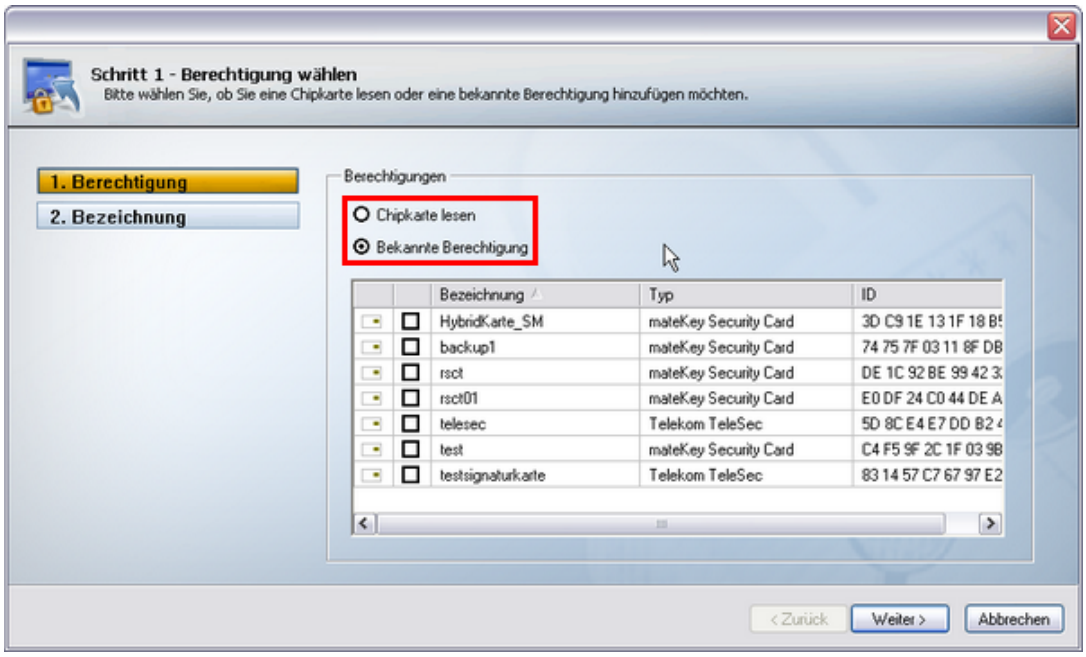
Als Wildcard können Sie ein ***** benutzen. Wenn Sie z.B. **PCEntw*** bei der Beschränkung verwenden, kann sich der Mitarbeiter an alle Computer anmelden, die **PCEntw** im Computernamen enthalten.

Bei der **erweiterten Anmeldung** kann login***Mate***® nach der Windows-Anmeldung einen weiteren Anmeldedialog (z.B. Anmeldung an einem Linux- oder Netzwerkserver) ausführen. Aktivieren Sie hierzu die erweiterte Anmeldung. Tragen Sie den Fenstertext des Anmeldedialogs und das

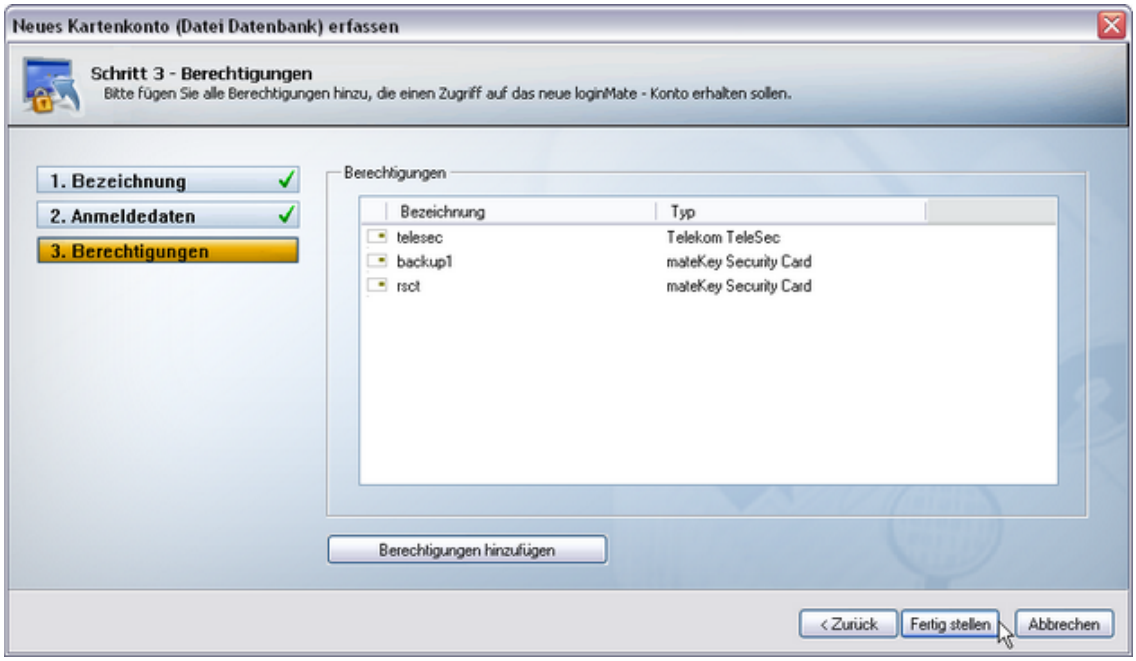
Passwort der Anmeldung ein.

3. Berechtigungen

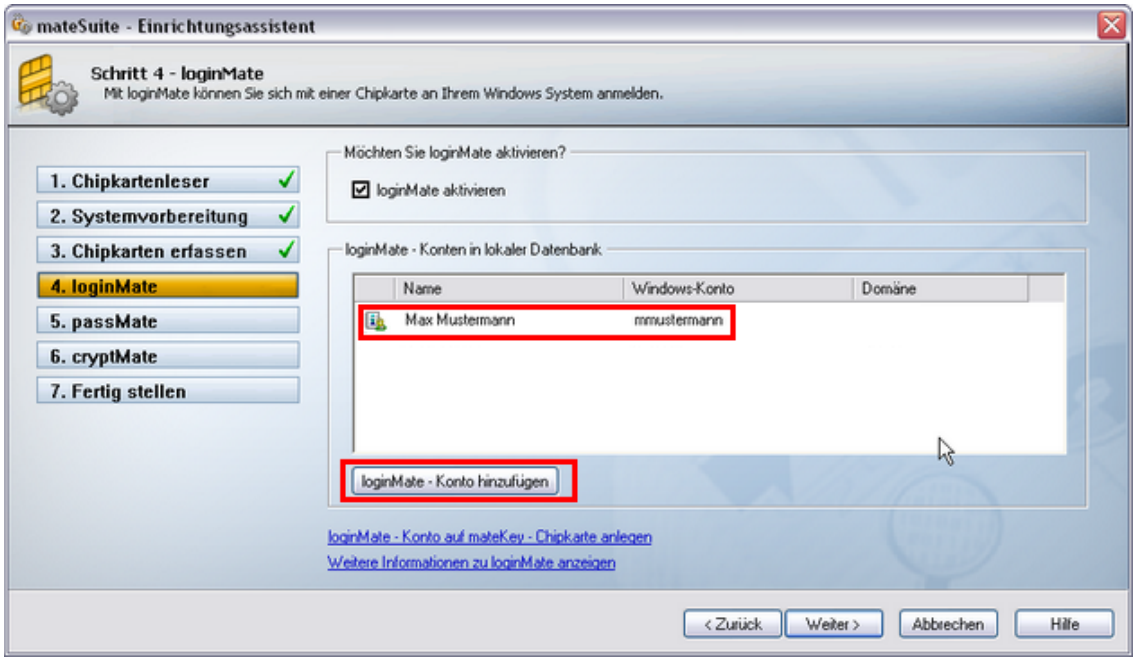
In diesem Schritt geben Sie die Berechtigungen an, die einen Zugriff auf das neue login***Mate***® Konto erhalten sollen.
Klicken Sie auf den **Button Berechtigungen hinzufügen** und Sie können die Berechtigungen für das Konto definieren.



Sie können die Berechtigung aus bereits erfassten Karten (Bekannte Berechtigung) oder Sie können eine neue Chipkarte (Chipkarte lesen) als Berechtigung hinzufügen. Die bekannten Berechtigungen können Sie in der Tabelle auswählen. Mit dem **Button Weiter** übernehmen Sie die Berechtigung für das neue Konto.
Bei **Chipkarte lesen** stecken Sie eine neue Karte in den Chipkartenleser und drücken ebenfalls **Weiter**. Folgen Sie dem Assistenten.



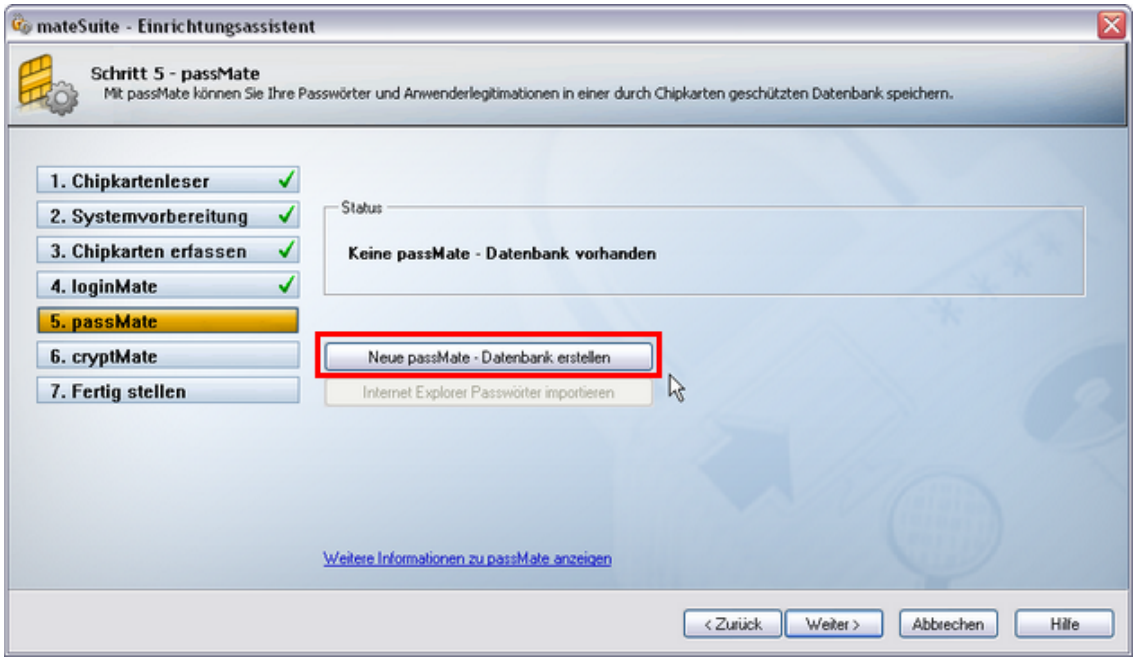
Sie sehen nun die hinzugefügten Berechtigungen für das login***Mate***® Konto. Bestätigen Sie mit Fertig stellen und das login***Mate***® Konto ist eingerichtet.



Mit dem **Button loginMate Konto** hinzufügen können Sie mehrere login***Mate***®-Konten auf einem PC einrichten, z.B ein Administrator- und ein Benutzerkonto.
Findet login***Mate***® beim Anmeldevorgang zu einer Chipkarte mehrere gültige Konten, wird ein entsprechendes Auswahlmenü angezeigt.

5.1.5 Schritt 5 - Einrichtung passMate

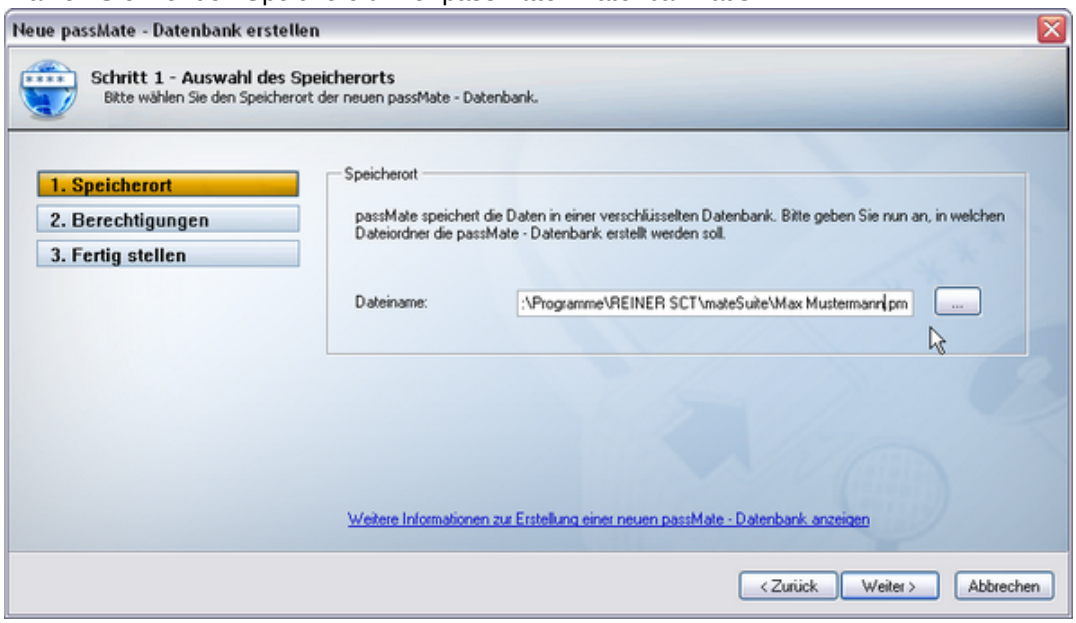
In diesem Schritt richten Sie eine pass***Mate***®-Datenbank ein. In dieser Datenbank werden dann alle Passwörter, die Sie anlegen werden, verschlüsselt gespeichert.



Klicken Sie auf den **Button Neue passMate-Datenbank erstellen**.

1. Auswahl des Speicherorts

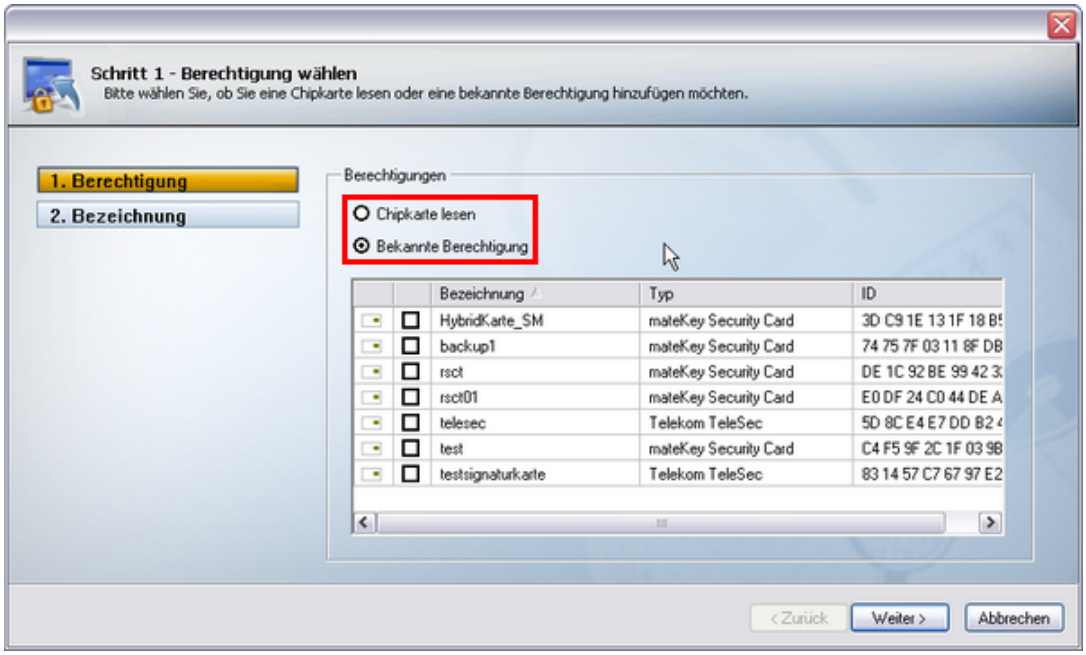
Wählen Sie hier den Speicherort Ihrer pass***Mate***®-Datenbank aus.


Neue passMate - Datenbank erstellen
Schritt 1 - Auswahl des Speicherorts
Bitte wählen Sie den Speicherort der neuen passMate - Datenbank.
1. Speicherort
2. Berechtigungen
3. Fertig stellen
Speicherort
passMate speichert die Daten in einer verschlüsselten Datenbank. Bitte geben Sie nun an, in welchen Dateiordner die passMate - Datenbank erstellt werden soll.
Dateiname:
:\Programme\REINER SCT\mateSuite\Max Mustermann.pm
...
Weitere Informationen zur Erstellung einer neuen passMate - Datenbank anzeigen
< Zurück
Weiter >
Abbrechen

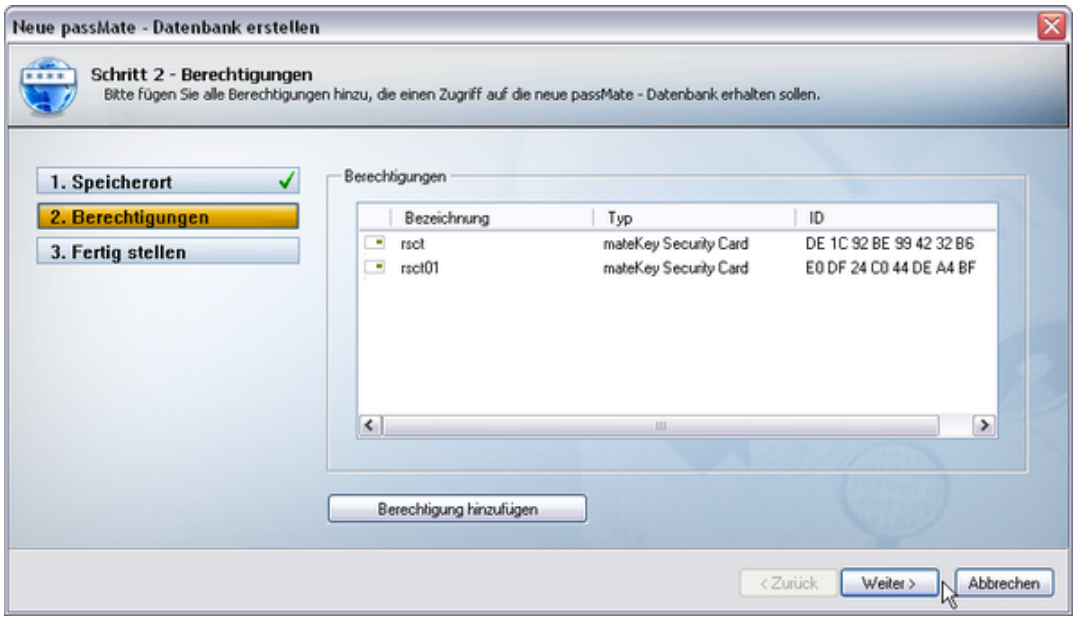
Anschließend müssen analog zur Einrichtung bei login***Mate***® die Berechtigungen hinzugefügt werden.

2. Berechtigungen

In diesem Schritt geben Sie die Berechtigungen an, die einen Zugriff auf das neue pass***Mate***® Datenbank erhalten sollen.
Klicken Sie auf den **Button Berechtigungen hinzufügen** und Sie können die Berechtigungen für das Konto definieren.

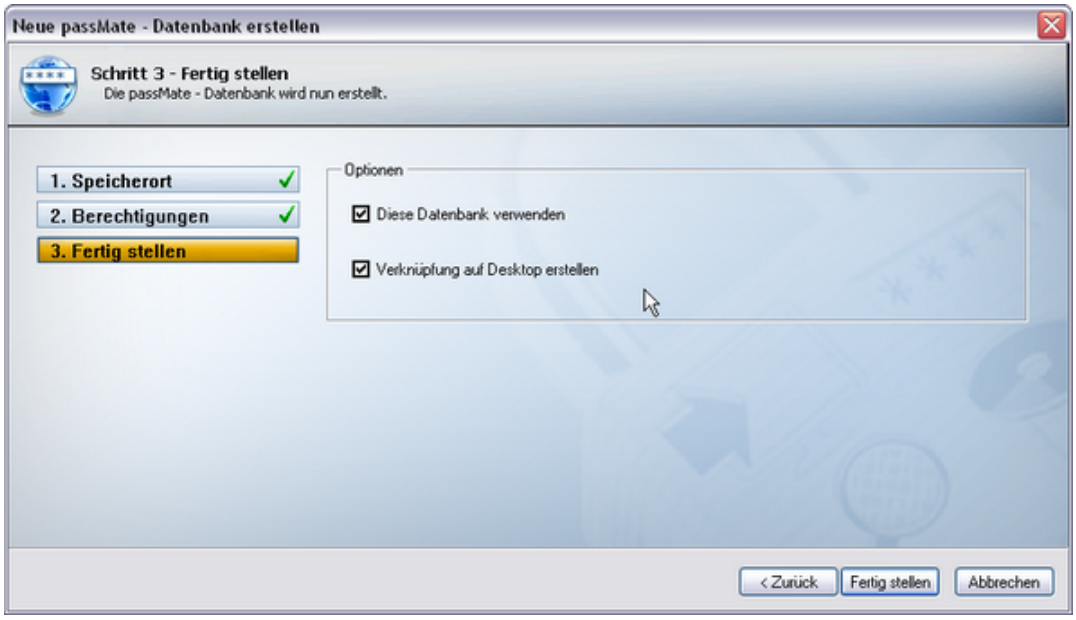


Sie können die Berechtigung aus bereits erfassten Karten (Bekannte Berechtigung) oder Sie können eine neue Chipkarte (Chipkarte lesen) als Berechtigung hinzufügen. Die bekannten Berechtigungen können Sie in der Tabelle auswählen. Mit dem **Button Weiter** übernehmen Sie die Berechtigung für das neue Konto.
Bei **Chipkarte lesen** stecken Sie eine neue Karte in den Chipkartenleser und drücken ebenfalls **Weiter**. Folgen Sie dem Assistenten.

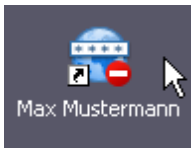


Hier sehen Sie die angelegten Berechtigungen. Klicken Sie auf **Weiter**.

3. Fertig stellen

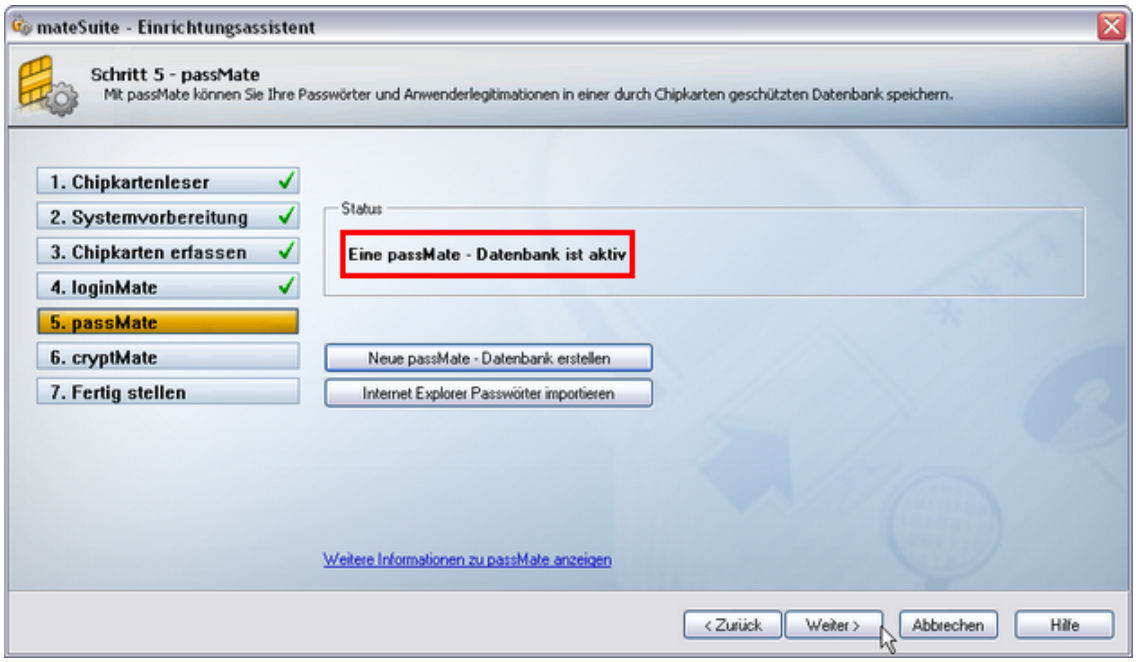


Hier können Sie die Optionen **Diese Datenbank verwenden** und **Verknüpfung auf Desktop erstellen** auswählen.



Mit der Verknüpfung auf dem Desktop können Sie die Datenbank per Maustaste öffnen oder schließen.

Wählen Sie die entsprechenden Optionen aus und bestätigen Sie mit **Fertig stellen**.



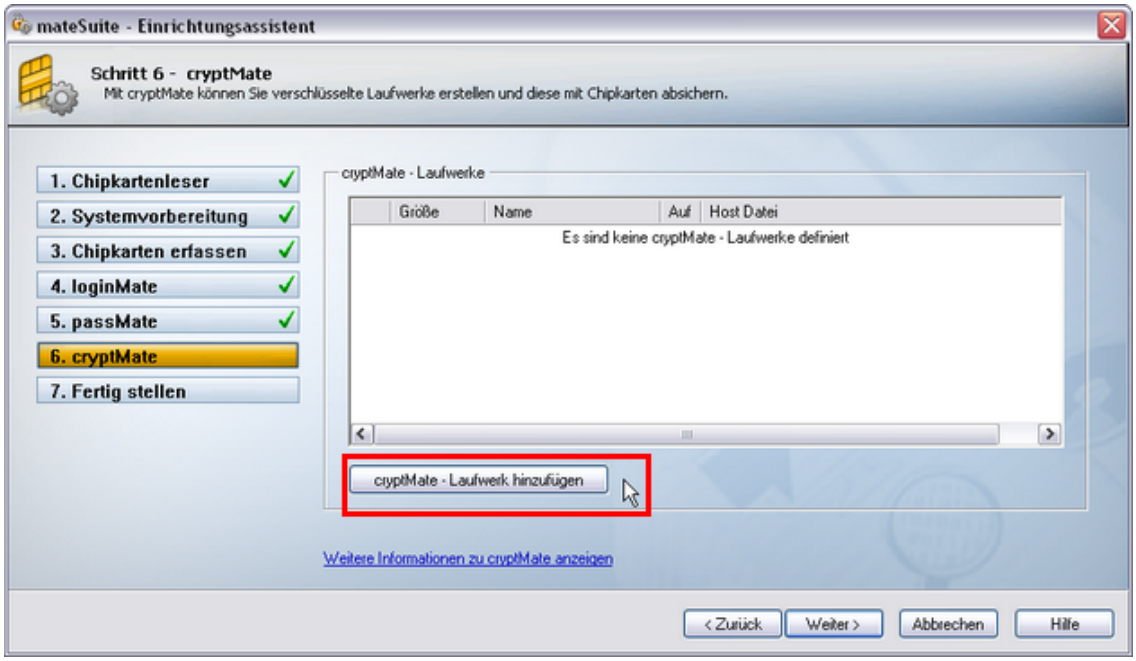
Es wurde nun eine aktive pass***Mate***® Datenbank angelegt.

Über den Button Internet *Explorer Passwörter importieren*, können die im Internet Explorer über die AutoVervollständigen-Funktion gespeicherten Internet-Passwörter in die sichere pass***Mate***®-

Datenbank importiert werden.

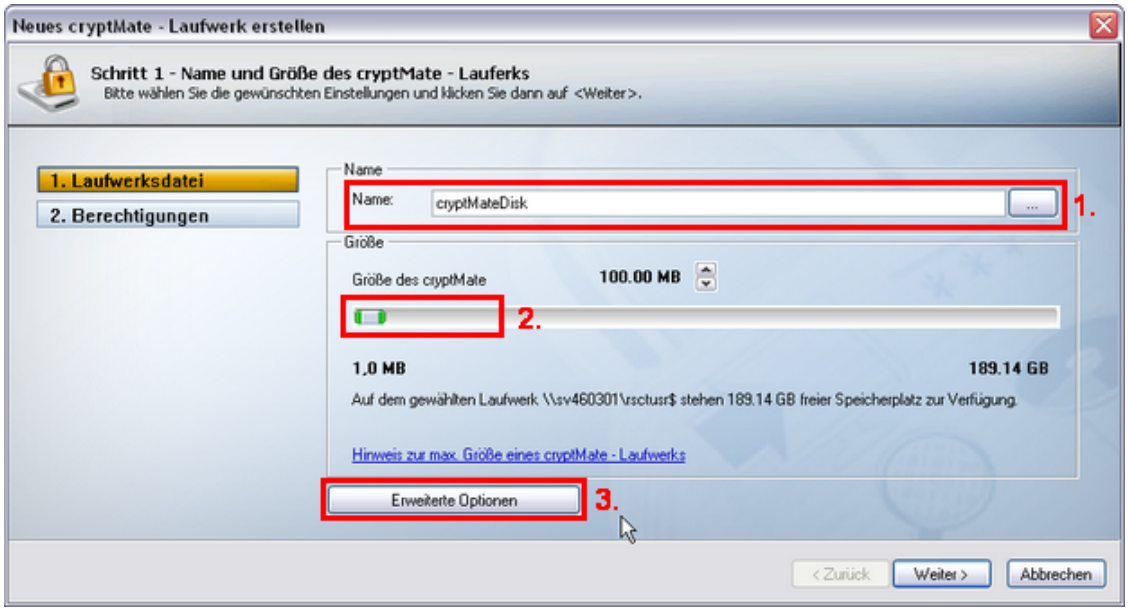
5.1.6 Schritt 6 - Einrichtung cryptMate

In diesem Schritt wird Ihnen das Einrichten eines crypt***Mate***®-Laufwerks beschrieben. Sie erstellen eine Laufwerksdatei auf Ihrem System und mit Hilfe dieser Laufwerksdatei wird das virtuelle Laufwerk gemountet.



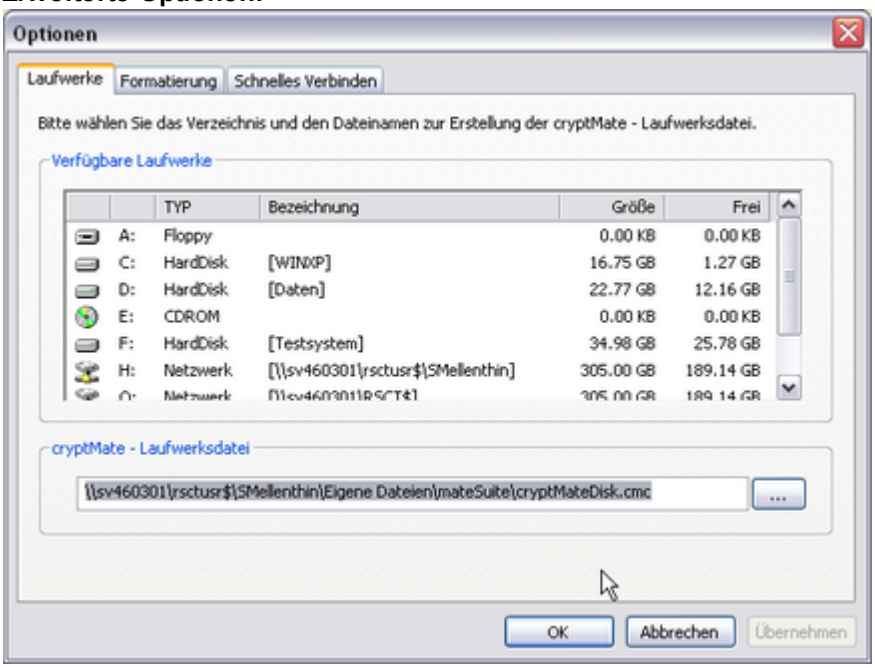
Klicken Sie auf den **Button cryptMate-Laufwerk** hinzufügen.

1. Name und Größe des cryptMate-Laufwerks

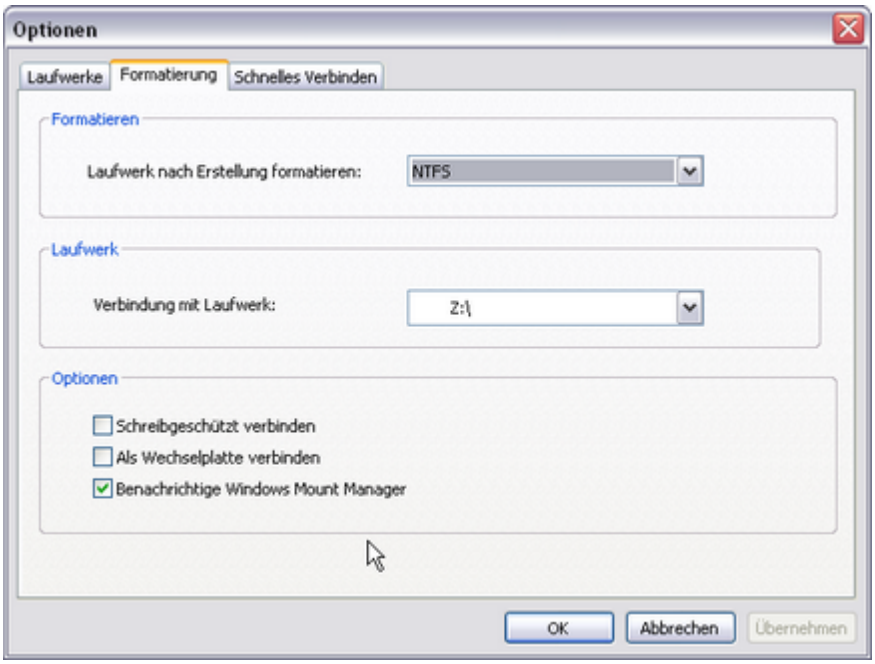


Bei Punkt (1) geben Sie den Namen und den Speicherort der cryptMate-Laufwerksdatei ein. Die Größe des cryptMate-Laufwerks können Sie mit den Reglern (2) festlegen. In den erweiterten Optionen (3) können Sie folgende Einstellungen vornehmen.

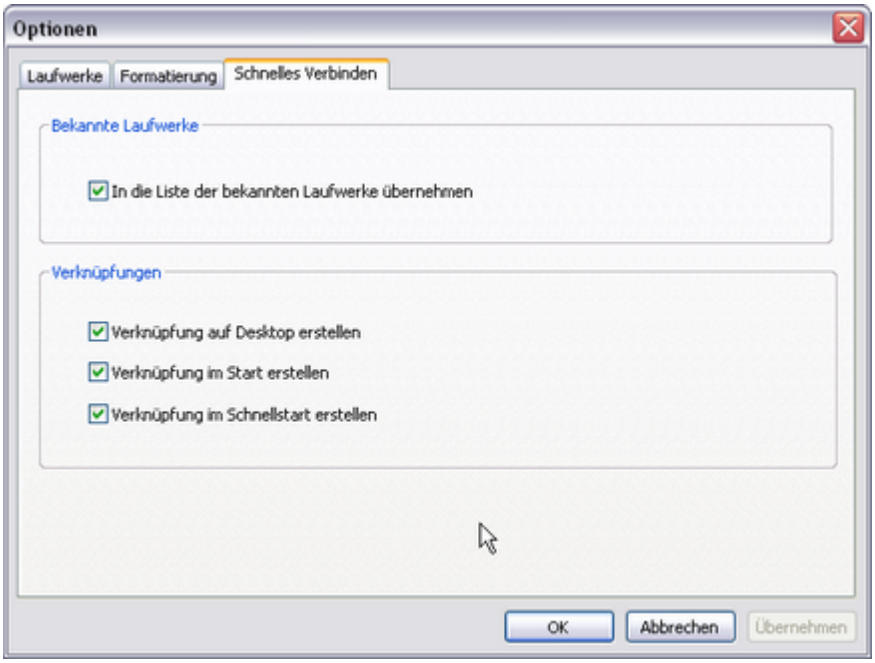
Erweiterte Optionen:



Beim Reiter Laufwerke können Sie den Zielort der cryptMate-Laufwerksdatei festlegen.



Beim Reiter Formatierung legen Sie die Formatierungsoption fest und weisen dem virtuellen Laufwerk einen Laufwerksbuchstaben zu. Folgende Optionen stehen zur Auswahl:
- Schreibgeschützt verbinden: Das gemountete Laufwerk ist schreibgeschützt.
- Als Wechselplatte verbinden: Das gemountete Laufwerk wird als Wechselplatte von Windows behandelt.
- Benachrichtige Windows Mount Manager: Die Option ist unbedingt zu wählen, da das erstellte Laufwerk in Windows sonst nicht angezeigt wird.



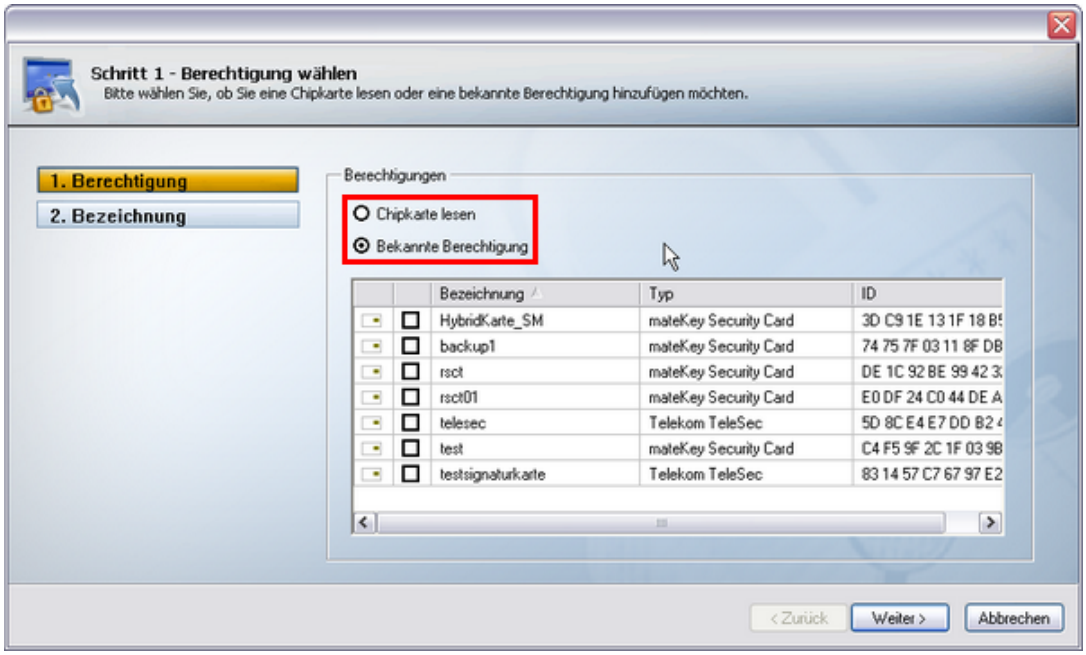
Im Reiter Schnelles Verbinden können Sie auswählen, ob das erstellte Laufwerk in die Liste der bekannten Laufwerke aufgenommen werden soll. Dies ist zu empfehlen, da das Handhaben der erstellten Laufwerke erleichtert wird.

Bei Verknüpfungen können Sie auswählen, wo eine Verknüpfung mit dem Laufwerk erstellt werden soll.

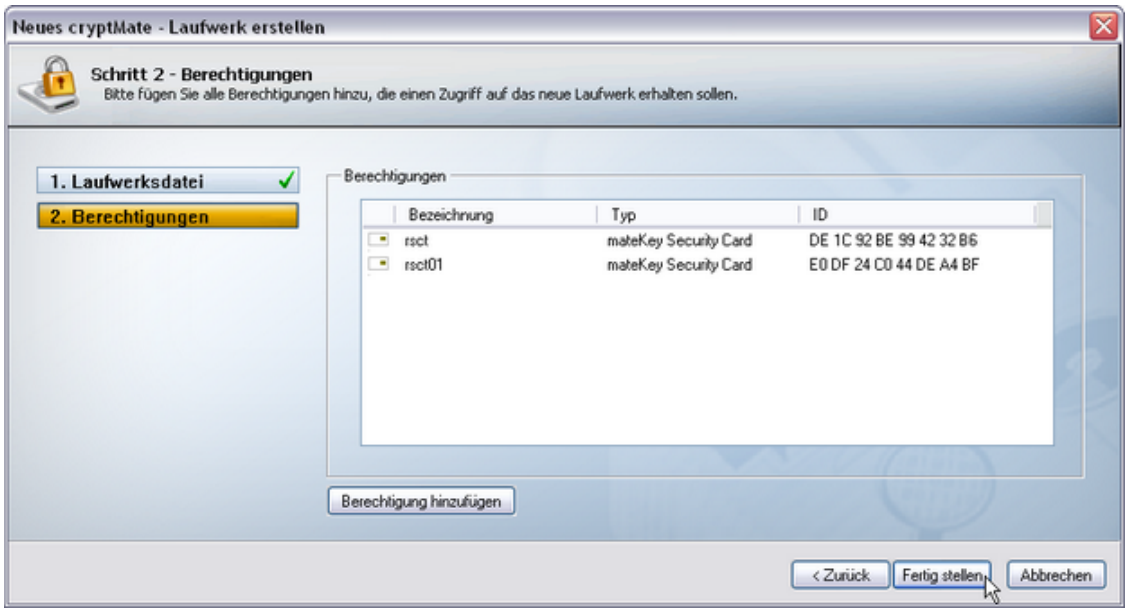
Mit der Verknüpfung auf dem Desktop können Sie mit der Maustaste das cryptMate-Laufwerk verbinden und wieder trennen.

2. Berechtigungen

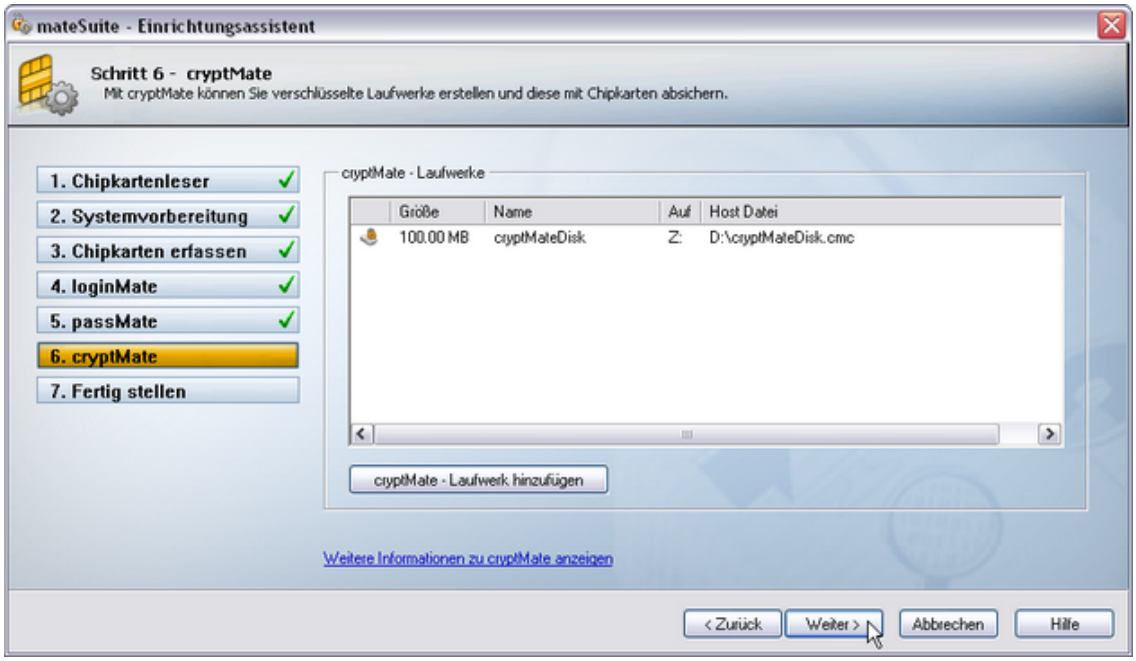
In diesem Schritt geben Sie die Berechtigungen an, die einen Zugriff auf das neue crypt***Mate***® Datenbank erhalten sollen.
Klicken Sie auf den **Button Berechtigungen hinzufügen** und Sie können die Berechtigungen für das Konto definieren.



Sie können die Berechtigung aus bereits erfassten Karten (Bekannte Berechtigung) oder Sie können eine neue Chipkarte (Chipkarte lesen) als Berechtigung hinzufügen. Die bekannten Berechtigungen können Sie in der Tabelle auswählen. Mit dem **Button Weiter** übernehmen Sie die Berechtigung für das neue Konto.
Bei **Chipkarte lesen** stecken Sie eine neue Karte in den Chipkartenleser und drücken ebenfalls **Weiter**. Folgen Sie dem Assistenten.



Hier sehen Sie die angelegten Berechtigungen. Klicken Sie auf **Fertig stellen**. Das crypt***Mate***®-Laufwerk wird formatiert und angelegt.



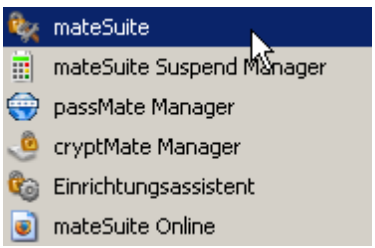
Sie sehen hier Ihr erstelltes Laufwerk. Klicken Sie auf Weiter und der Einrichtungsassistent wird beendet und Sie können den mateSuite-Administrator starten.

5.2 mateSuite-Administrator

Der mate***Suite***-Administrator ist das zentrale Steuerungs- und Administrationstool aller mate***Suite***-Anwendungen und Services.

Der Aufruf erfolgt über das mate***Suite***-Icon auf dem Desktop

oder alternativ über das Windows Startmenü unter **Start | Programme | REINER SCT mateSuite.**



5.2.1 mateSuite-Anwendungen

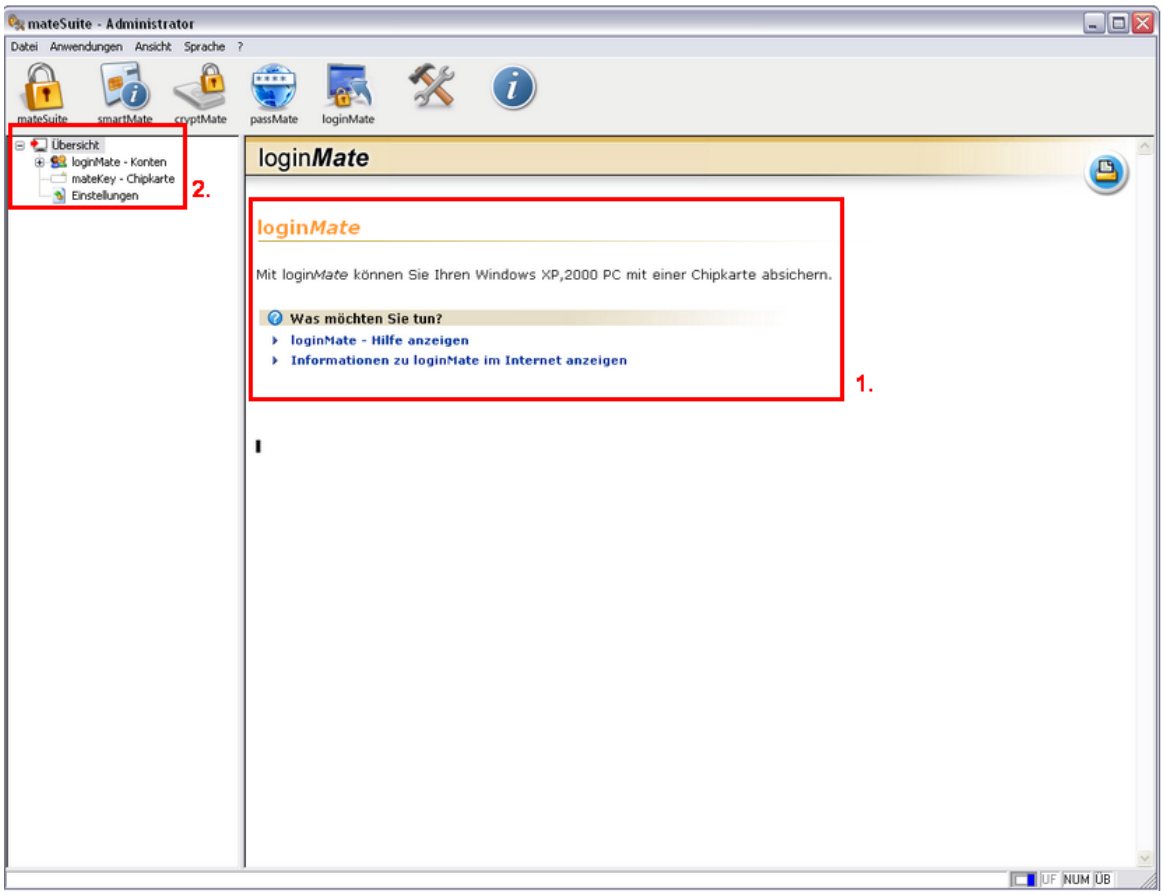
mate***Suite*** integriert verschiedene Sicherheitsanwendungen für Chipkarten und Chipkartenleser. Mit Hilfe von mate***Suite*** können Sie Ihre Chipkarte multifunktional nutzen: Vom Auslesen der Karte, über das sichere Verwalten von Passwörtern, bis hin zur Verschlüsselung von Laufwerken, bietet mate ***Suite*** ein breites Spektrum an Datenschutz- und Sicherheitsfunktionalität für Ihre Rechnerumgebung.

login***Mate***®	**Login mit Chipkarten für Windows 2000/XP/2003 Server**
crypt***Mate***®	**Speicherung vertraulicher und sensibler Daten auf speziell verschlüsselten virtuellen Laufwerken**
pass***Mate***®	**Verwaltung beliebiger PC- und Internet-Zugangsberechtigungen**
smart***Mate***®	**Anzeigen und Bearbeiten von Daten verschiedener Chipkarten**

5.2.1.1 loginMate

Mit login***Mate***® können Sie Ihren Windows 2003 Server-/XP-/2000-PC mittels Chipkartentechnologie absichern. Hierfür übernimmt login***Mate***® die Steuerung der Windows-Anmeldung. Anstatt einer Passworteingabe, wird der PC mit einer Chipkarte freigeschaltet.

Um mit loginMate zu arbeiten, starten Sie mateSuite und klicken den Button loginMate.



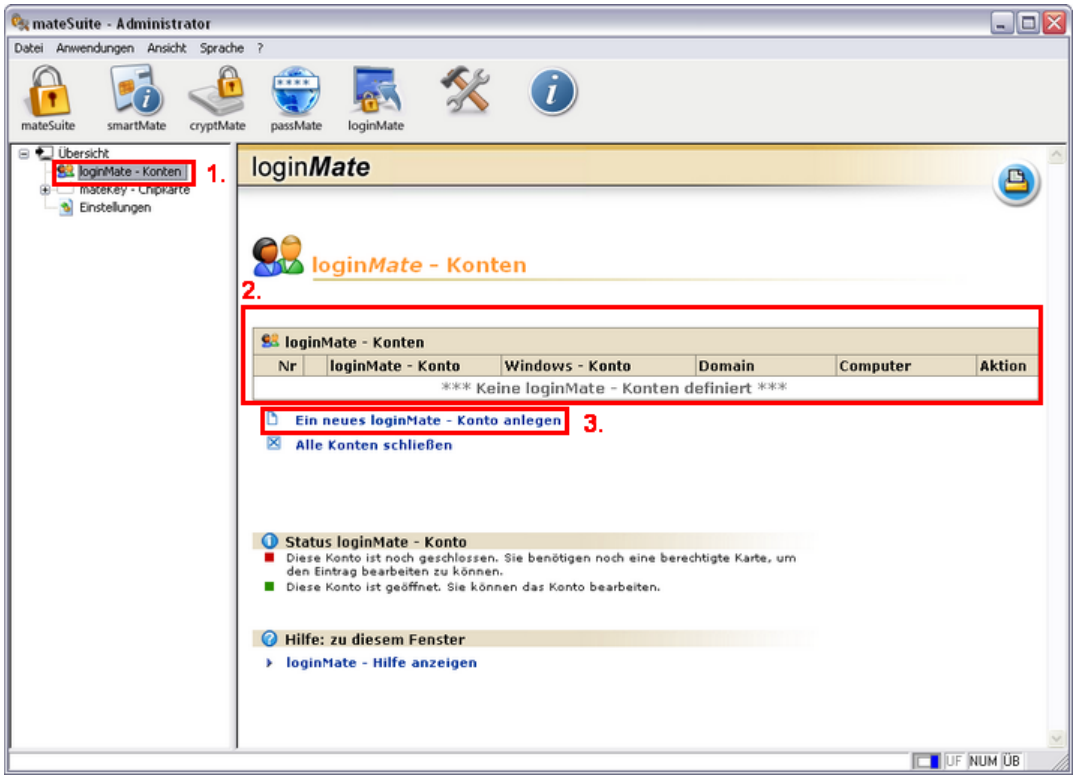
Im Bereich (1) können Sie die Einstellungen zu den loginMate-Konten vornehmen. Auf der linken Seite (2) stehen folgenden Optionen zur Auswahl:

loginMate - Konten: Erstellen und bearbeiten neuer oder vorhandener loginMate Konten in einer lokalen Datei.
mateKey - Chipkarte: Erstellen und bearbeiten neuer oder vorhandener loginMate Konten auf einer mateKey - Chipkarte
Einstellungen: Bearbeiten der login - Einstellungen.

5.2.1.1.1 Konten erstellen

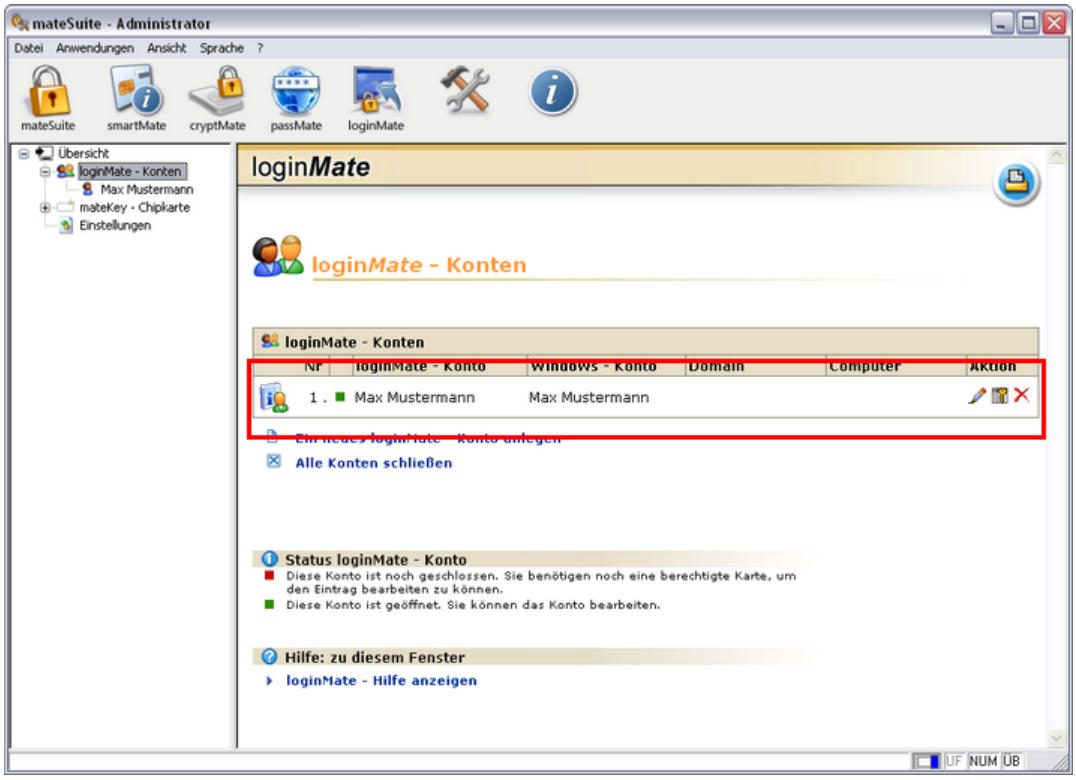
loginMate-Konto in einer Datei Datenbank schreiben

Um ein neues Konto anzulegen, gehen Sie links auf *loginMate-Konten* (1).



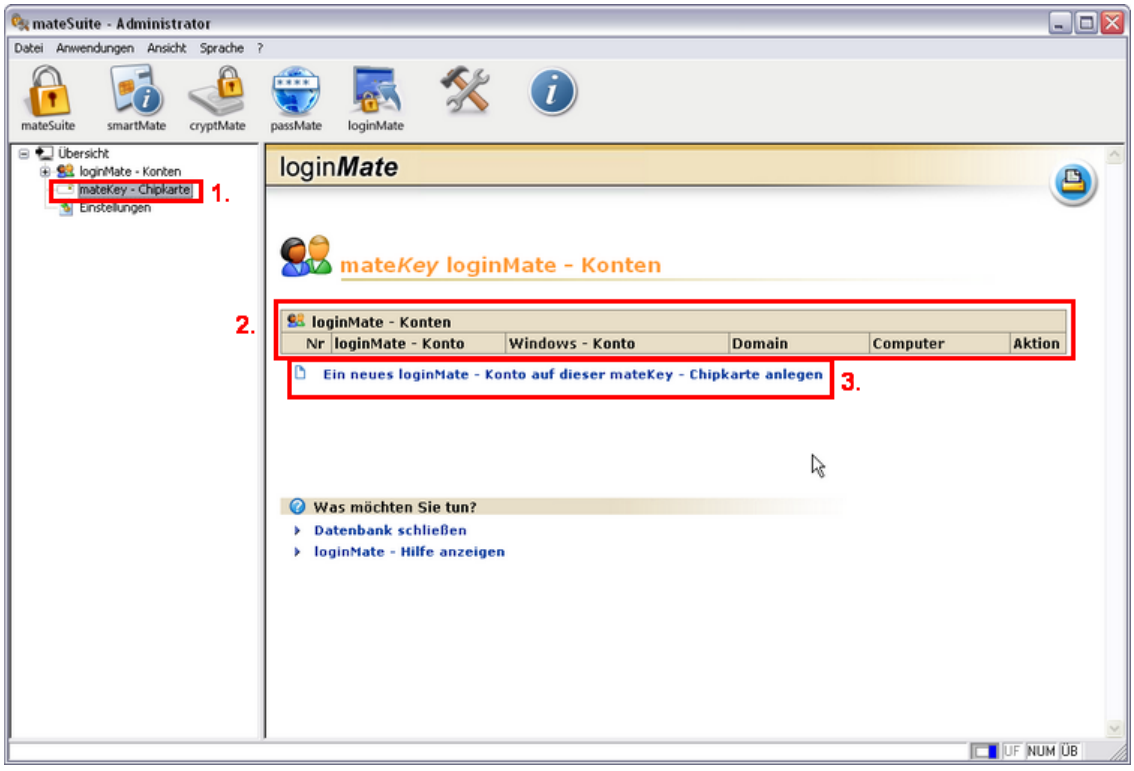
Beim Punkt (2) sehen Sie alle vorhandenen Konten. Um ein neues Konto anzulegen, drücken Sie *Ein neues loginMate-Konto anlegen* (3). Der folgende Ablauf ist identisch mit der Einrichtung im Einrichtungsassistenten im Schritt 4.

Wenn Sie alle Schritte ausgeführt haben, erscheint das Konto bei den loginMate-Konten.



loginMate-Konto auf eine mateKey-Chipkarte erfassen

Um ein neues Konto anzulegen, gehen Sie links auf *mateKey-Chipkarte* (1).



Beim Punkt (2) sehen Sie alle vorhandenen Konten auf dieser Chipkarte. Um ein neues Konto anzulegen, drücken Sie *Ein neues loginMate-Konto auf dieser mateKey-Chipkarte anlegen* (3). Der folgende Ablauf ist identisch mit der Einrichtung im Einrichtungsassistenten im Schritt 4.

Wenn Sie alle Schritte ausgeführt haben, erscheint das Konto bei den mate***Key*** loginMate-Konten. Sie brauchen für dies Art Konto keine zusätzlichen Berechtigungen definieren, da das Konto schon auf einer eigenen Chipkarte angelegt wurde.

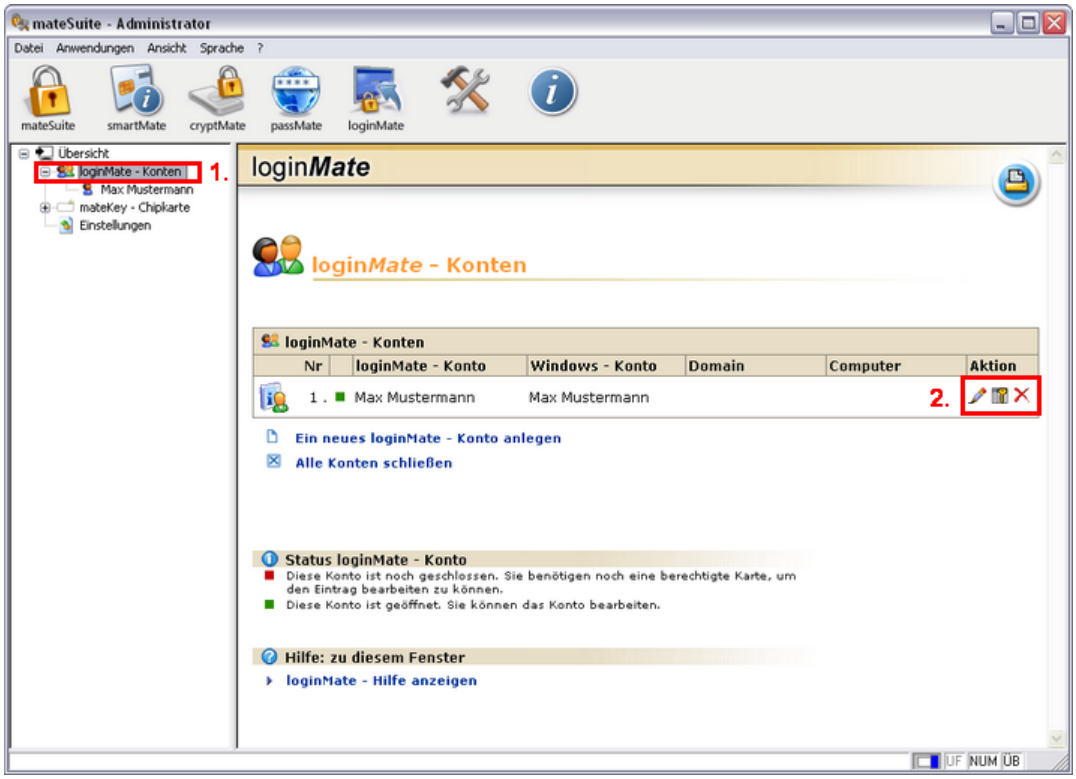
5.2.1.1.2 Kontenverwaltung

Die login***Mate***®-Kontenverwaltung bietet folgende Funktionen:

- login***Mate***®-Konten anzeigen
- Neue login***Mate***®-Konten anlegen
- login***Mate***®-Konten bearbeiten
- login***Mate***®-Konten löschen
- Passwörter zu login***Mate***®-Konten ändern
- Berechtigungen zu login***Mate***®-Konten vergeben bzw. löschen
- Einstellungen zu login***Mate***®-Konten vornehmen

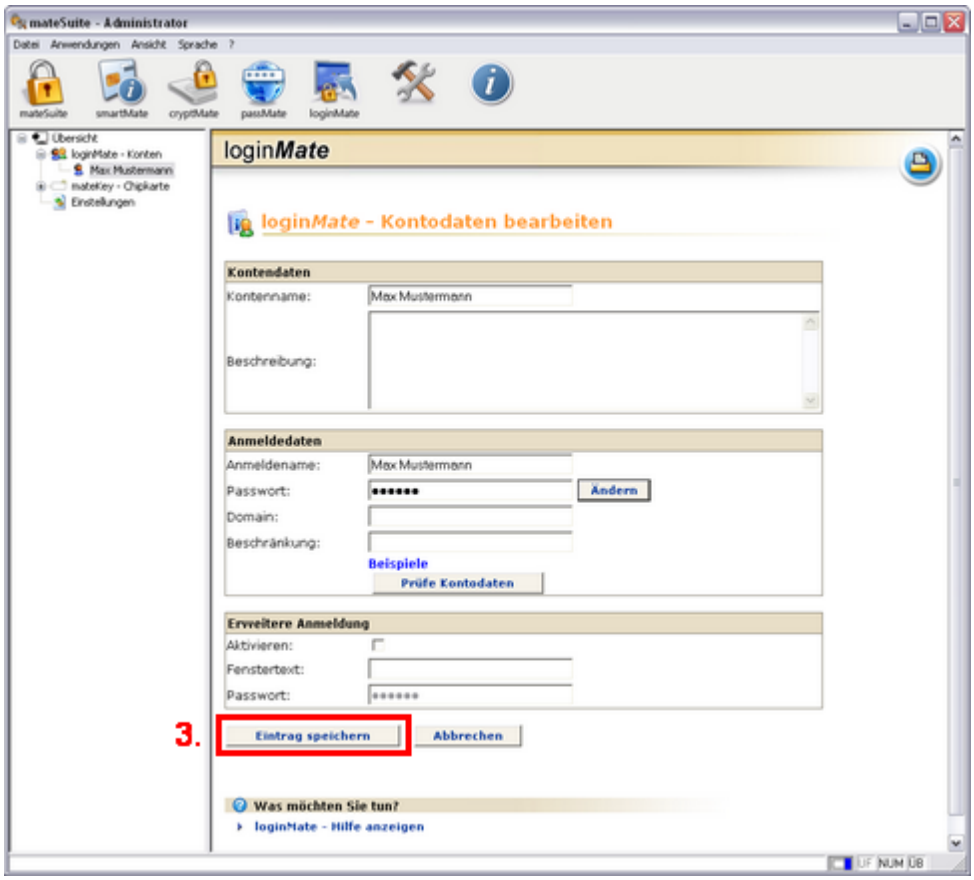
Kontenansicht

Wenn Sie links auf *loginMate/Konten* (1)klicken, sehen Sie welche Konten Sie eingerichtet haben.



login*Mate*®-Konten bearbeiten

Klicken Sie auf den **Stift** (2), um das Konto zu bearbeiten.

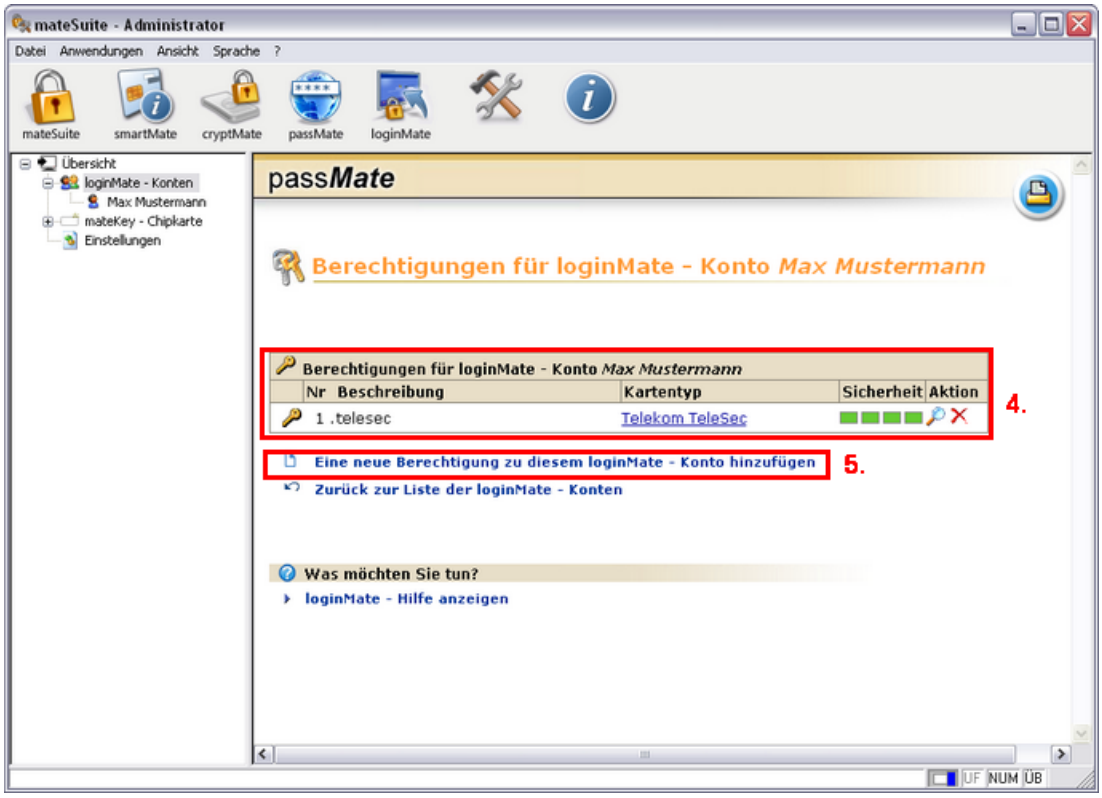


Hier können Sie alle Änderungen vornehmen. Bestätigen Sie Ihre Änderungen mit dem **Button Eintrag speichern** (3).

Mit dem Kreuz (2) können Sie vorhandene Konten löschen.

Berechtigungen vergeben/löschen

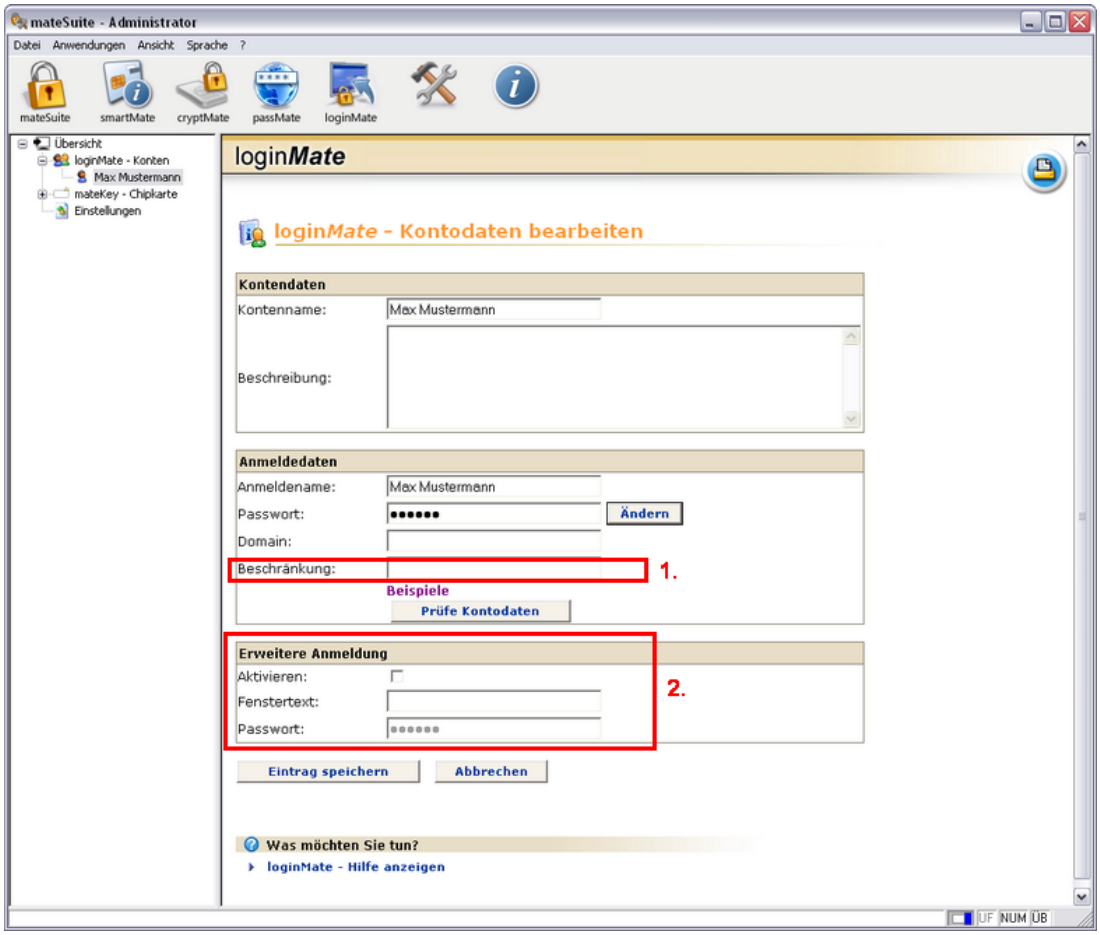
Um Berechtigungen für die Konten hinzuzufügen, klicken Sie auf das -Symbol (2).



Sie sehen hier alle zu diesem Konto vorhandenen Berechtigungen (4). Um weitere Berechtigungen hinzuzufügen, klicken Sie *Eine neue Berechtigung zu diesem loginMate - Konto hinzufügen* (5). Der folgende Ablauf ist identisch mit dem Hinzufügen der Berechtigung im Einrichtungsassistenten im Schritt 4. Mit dem Kreuz ✕ können Sie vorhandene Berechtigungen wieder entfernen.

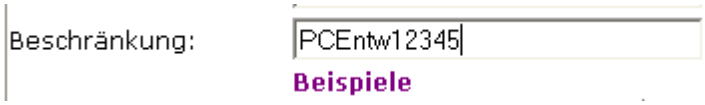
5.2.1.1.3 Kontenbeschränkung/Erweiterte Anmeldung

Sie haben die Möglichkeit Ihre login***Mate***® Konten verschiedenen Rechnern zuzuordnen. Hierzu weisen Sie den einzelnen Konten Beschränkungen zu.



Bei **Beschränkung** (1)können Sie anhand des Computernamens Ihre login***Mate***® Konten verschiedenen Rechnern zuordnen. Hierzu weisen Sie den einzelnen Konten Beschränkungen zu. Sie können diese Beschränkungen bereits bestehenden Konten oder neuen Konten zuweisen.

Beispiel:
Sie haben einen PC mit dem Computernamen **PCEntw12345**. Jetzt soll der Mitarbeiter sich nur an diesem Computer anmelden dürfen. Dazu tragen Sie den Computernamen der Arbeitsstation bei Beschränkungen ein.



Als Wildcard können Sie ein * benutzen. Wenn Sie z.B. **PCEntw*** bei der Beschränkung verwenden, kann sich der Mitarbeiter an alle Computer anmelden, die **PCEntw** im Computernamen enthalten.

Bei der **erweiterten Anmeldung** (2) kann login***Mate***® nach der Windows-Anmeldung einen weiteren Anmeldedialog (z.B. Anmeldung an einem Linux- oder Netzwerkserver) ausführen. Aktivieren Sie hierzu die erweiterte Anmeldung. Tragen Sie den Fenstertext des Anmeldedialogs und das Passwort der Anmeldung ein.

5.2.1.1.4 Anmelden/Abmelden/Sperren/Entsperren

Im folgenden Kapitel werden Ihnen die verschiedenen Einsatzmöglichkeiten von login***Mate***® aufgezeigt.
Um die Funktionen von login***Mate***® zu nutzen, müssen Sie unter Einstellungen login*Mate* aktivieren.
Siehe Einstellungen.

5.2.1.1.4.1 Anmeldung

Wenn Sie nur ein Benutzerkonto erstellt haben, werden Sie beim Windowsstart nach der PIN gefragt.

cyberJack - Sichere PIN Eingabe
cyberJack - Sichere PIN Eingabe
Bitte geben Sie Ihre PIN an der Tastatur des Lesers ein und bestätigen Sie mit OK.
PIN: _
Abbruch in 9 Sekunden

PIN-Eingabe beim cyberJack pinpad

PIN-Aufforderung beim cyberJack e-com

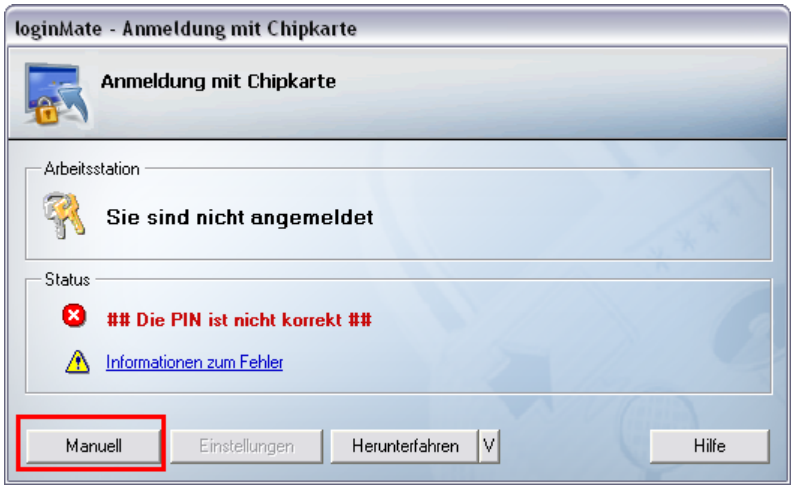
Geben Sie diese ein und bestätigen mit der Grünen **OK-Taste.**

Windows setzt seinen Bootvorgang fort.

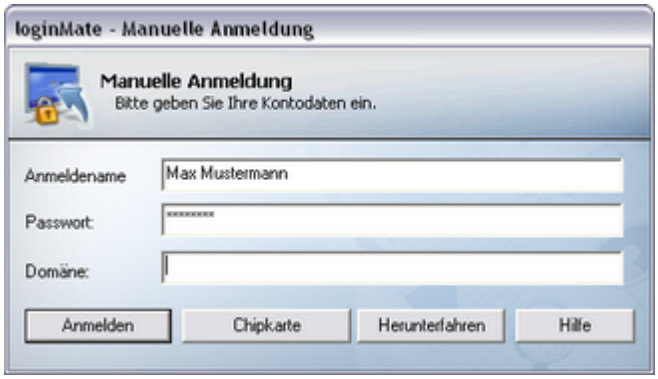
Bei Eingabe einer falschen PIN werden Sie gebeten die Chipkarte zu entfernen und wieder einzuführen.

Bitte geben Sie die richtige PIN ein und der Rechner beendet seinen Bootvorgang.

Wenn Sie Ihre PIN vergessen sollten, haben Sie die Möglichkeit sich manuell am System anzumelden.



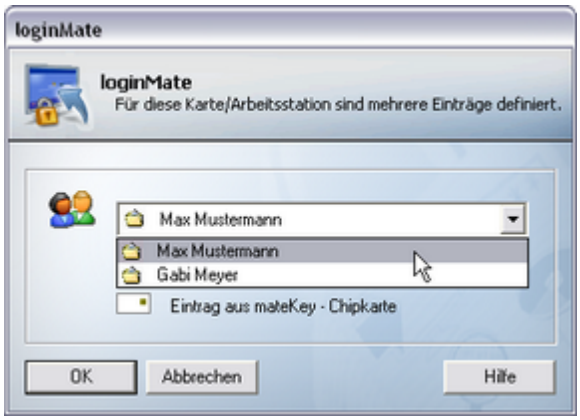
Klicken Sie den **Button Manuell**.



Nun können Sie Ihr Windowskonto manuell eingeben und somit den PC starten.

5.2.1.1.4.2 Benutzerkonto wählen

Wenn Sie mehrere Benutzerkonten definiert haben (Siehe Konten erstellen) und login***Mate*** unter Einstellungen aktiviert ist, dann können Sie sich beim Windowsstart das entsprechende Benutzerkonto auswählen, mit dem Sie sich anmelden möchten.



Wenn Sie mit **OK** bestätigen, werden Sie im nächsten Fenster nach der PIN Ihrer Chipkarte gefragt. Geben Sie diese ein und bestätigen mit der Grünen **OK-Taste.**

cyberJack - Sichere PIN Eingabe
cyberJack - Sichere PIN Eingabe
Bitte geben Sie Ihre PIN an der Tastatur des Lesers ein und bestätigen Sie mit OK.
PIN: _
Abbruch in 9 Sekunden

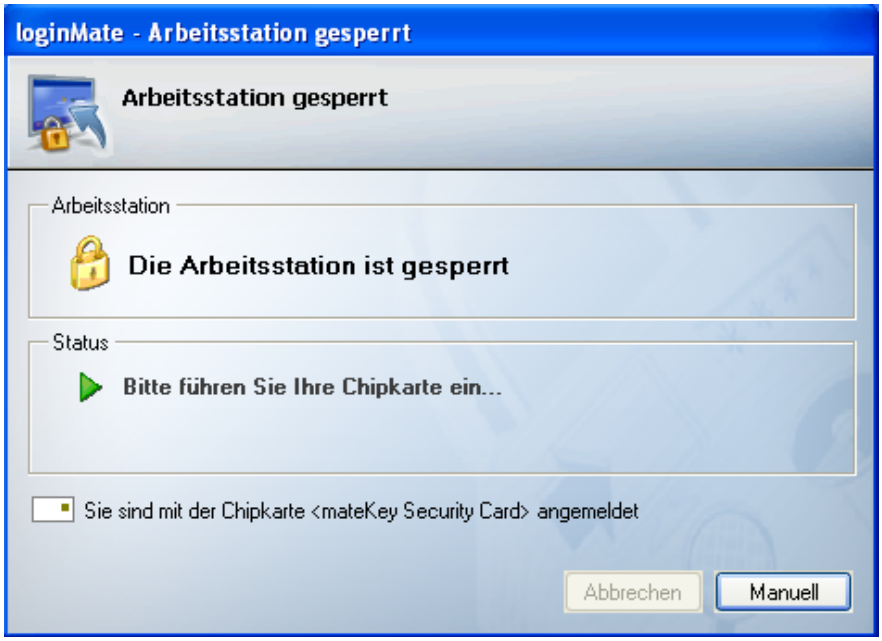
5.2.1.1.4.3 Sperren

Sperren mit Chipkarte

Um die Arbeitsstation mit einer Chipkarte zu sperren und anschließen wieder zu entsperren, muss unter Einstellungen die Haken bei *Automatisches Sperren der Arbeitsstation durch Entfernen der Chipkarte* und *Entsperren der Arbeitsstation mit Chipkarte* setzen.

Wenn Sie die Chipkarte entfernen, erscheint folgendes Bild und die Arbeitsstation ist gesperrt.

Entfernen Sie die Chipkarte. Nun ist der PC gesperrt und kann erst wieder durch Einführen der Karte entsperrt werden.



Nach Einführen der Karte werden Sie aufgefordert die PIN einzugeben.

cyberJack - Sichere PIN Eingabe
cyberJack - Sichere PIN Eingabe
Bitte geben Sie Ihre PIN an der Tastatur des Lesers ein und bestätigen Sie mit OK.
PIN: _
Abbruch in 9 Sekunden

PIN-Eingabe beim cyberJack pinpad

PIN-Aufforderung beim cyberJack e-com

Wenn Sie die korrekte PIN eingegeben haben wird der Rechner wieder entsperrt und Sie können weiter arbeiten.

Manuelle Sperrung

Die Arbeitsstation kann auf folgende Arten manuell gesperrt werden:

- Anklicken des mateSuite Suspend Managers mit der rechten Maustaste und Aktivieren der Funktion *Arbeitsstation sperren*
- Anklicken des mateSuite Suspend Managers mit der linken Maustaste + STRG-Taste

Es erscheint folgendes Fenster.

Entfernen Sie die Chipkarte und Ihr Rechner ist gesperrt.
Wenn Sie den Rechner entsperren möchten, führen Sie die Chipkarte ein und geben Sie anschließend die PIN ein.

cyberJack - Sichere PIN Eingabe
cyberJack - Sichere PIN Eingabe
Bitte geben Sie Ihre PIN an der Tastatur des Lesers ein und bestätigen Sie mit OK.
PIN: _
Abbruch in 9 Sekunden

PIN-Eingabe beim cyberJack pinpad

PIN-Aufforderung beim cyberJack e-com

Nach korrekter PIN Eingabe ist der Rechner entsperrt.

5.2.1.1.4.4 Runterfahren

Runterfahren mit Chipkarte

Um Ihren Rechner nur bei eingesteckter Chipkarte runterzufahren, gehen Sie wie folgt vor:

- Unter Einstellungen können Sie den Haken *Herunterfahren/Neustart der Arbeitsstation nur mit Chipkarte* aktivieren.
- Der Haken *Automatisches Sperren der Arbeitsstation durch Entfernen der Chipkarte* muss deaktiviert sein, sonst sperrt der Rechner beim Ziehen der Karte.

Jetzt können Sie Ihre Chipkarte im Windows Betrieb ziehen und beim Beenden von Windows werden Sie aufgefordert die Chipkarte, die Sie auch bei der Anmeldung verwendet haben, einzuführen.

Führen Sie die Chipkarte ein und der Rechner fährt runter.

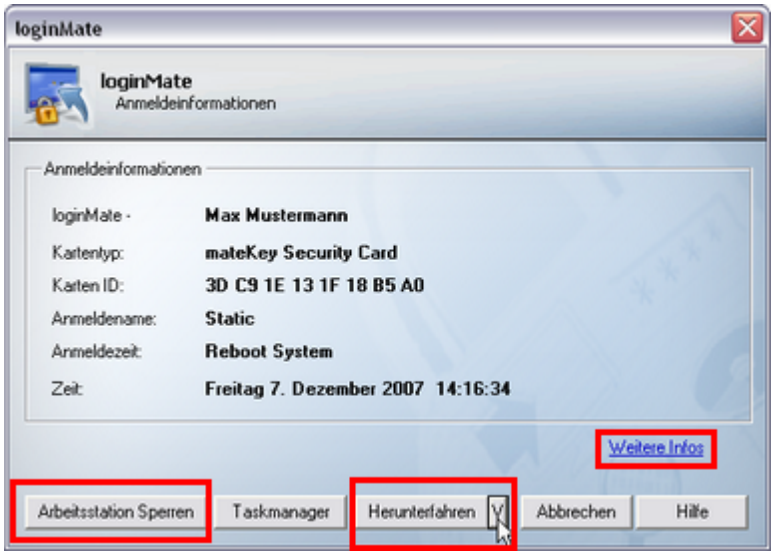
Manuelles Runterfahren

Um den Computer ohne Chipkarte herunterzufahren, deaktivieren Sie den Haken *Herunterfahren/ Neustart der Arbeitsstation nur mit Chipkarte* unter Einstellungen.

Jetzt können Sie den Rechner über **Start > Herunterfahren** beenden.

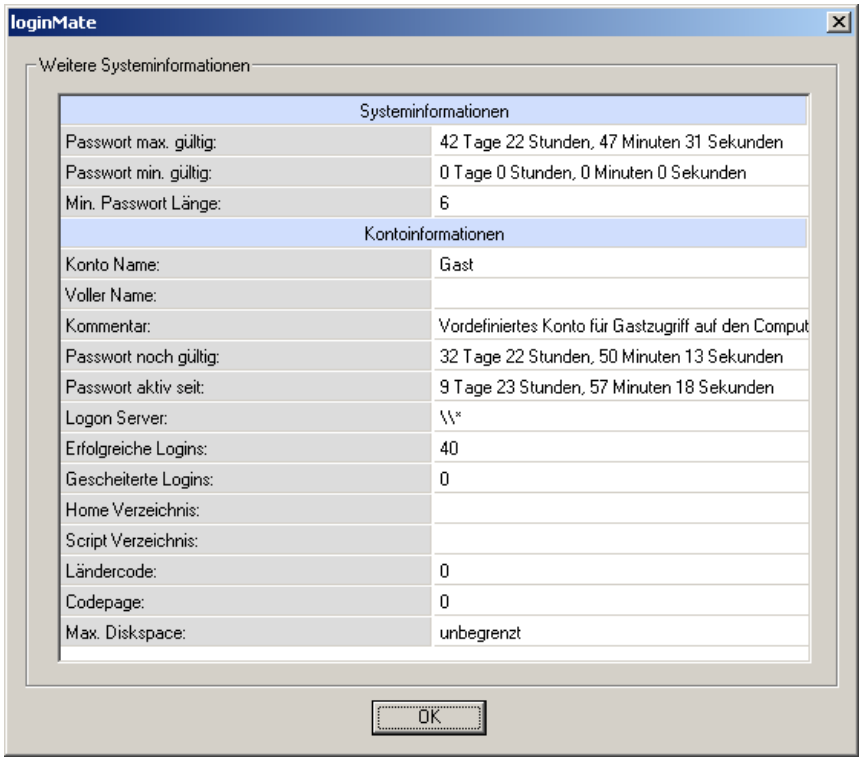
5.2.1.1.4.5 Funktion STRG+ALT+ENTF

Über die Tastenkombination STRG+ALT+Entfernen erhalten Sie folgendes Fenster, mit dem Sie bequem und schnell Informationen und einige Funktionen erreichen.

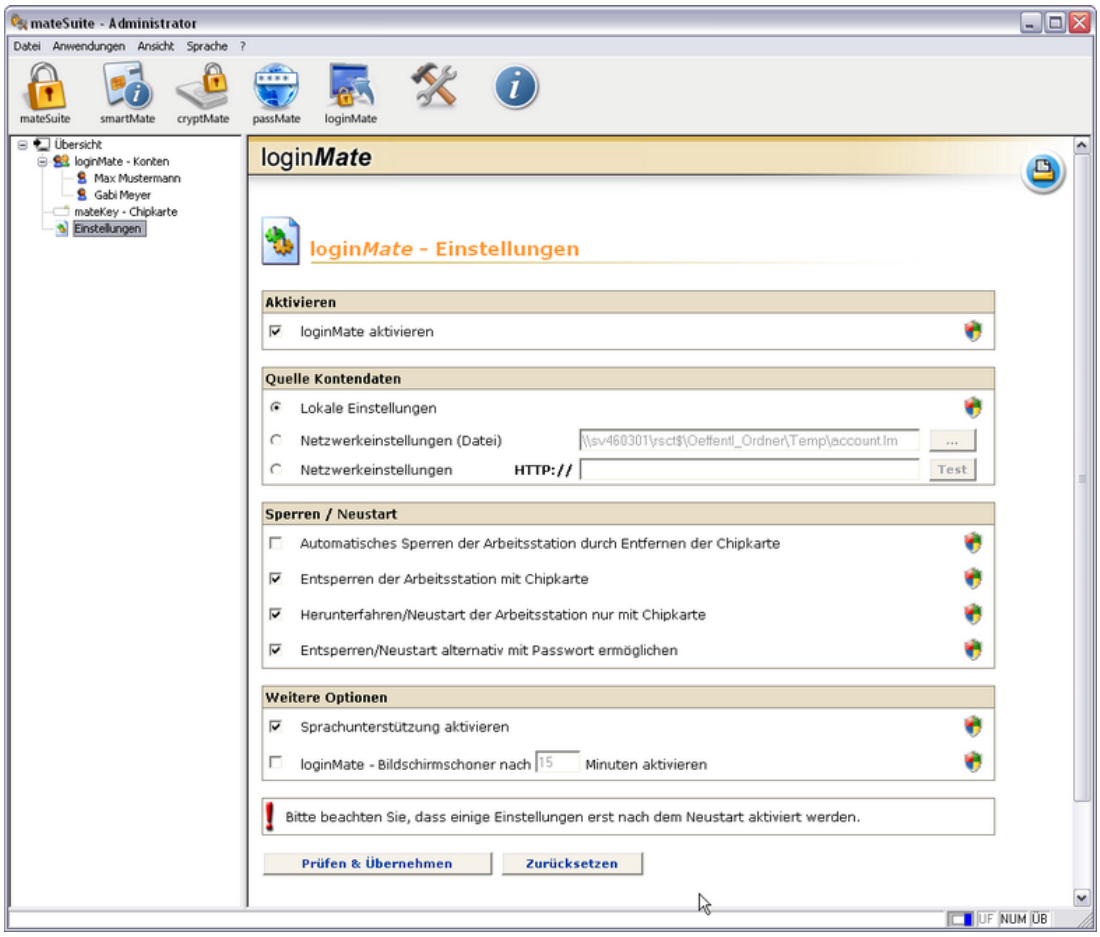


Hier werden Ihnen Informationen zum Konto und zur Karte angezeigt.

Außer dem können Sie über den Button **Arbeitsstation Sperren** den Rechner sperren.
Über den Button **Herunterfahren** stehen Ihnen die verschiedenen Windows-Abmeldungen zur Verfügung.
Über **Weitere Infos** erhalten Sie zusätzliche Informationen bezüglich Ihres Systems.



5.2.1.1.5 Einstellungen



Aktivieren

login***Mate***® lässt sich aktivieren und deaktivieren. Ist die Option *loginMate aktivieren* nicht aktiviert, startet der PC ohne login***Mate*** Unterstützung. Eine Anmeldung über Chipkarte ist in diesem Fall nicht mehr möglich.

Quelle Kontodaten

Wenn login***Mate***® innerhalb eines Netzwerkes genutzt wird und die login***Mate***®-Konten auf einem Netzwerklaufwerk gespeichert sind, muss der Netzwerkpfad zu den Kontodaten angeben werden.

Sperren/ Neustart

Wenn Sie das erste Kontrollkästchen *Automatisches Sperren der Arbeitsstation durch Entfernen der Chipkarte* aktivieren, dann wird der PC gesperrt, wenn die Chipkarte aus dem Chipkartenleser gezogen wird.

Die Aktivierung des zweiten Kontrollkästchens *Entsperren der Arbeitsstation mit Chipkarte* bewirkt, dass sich der PC mit der Chipkarte entsperren lässt.

Wenn Sie das dritte Kontrollkästchen *Herunterfahren/Neustart der Arbeitsstation nur mit Chipkarte* aktivieren, dann kann der Rechner **nur** mit Chipkarte neu starten oder runtergefahren werden. Sowohl Neustart als auch Abmeldung sind damit Passwort bzw. Chipkarten geschützt.

Bei Aktivierung von *Entsperren/Neustart alternativ mit Passwort ermöglichen* erfolgt die Freigabe des PC optional, mit SmartCard **oder** durch den manuellen Windows-Login.

Weitere Optionen

Wenn die Sprachunterstützung aktiviert ist, werden Sie verbal zur Eingabe der Chipkarte aufgefordert.

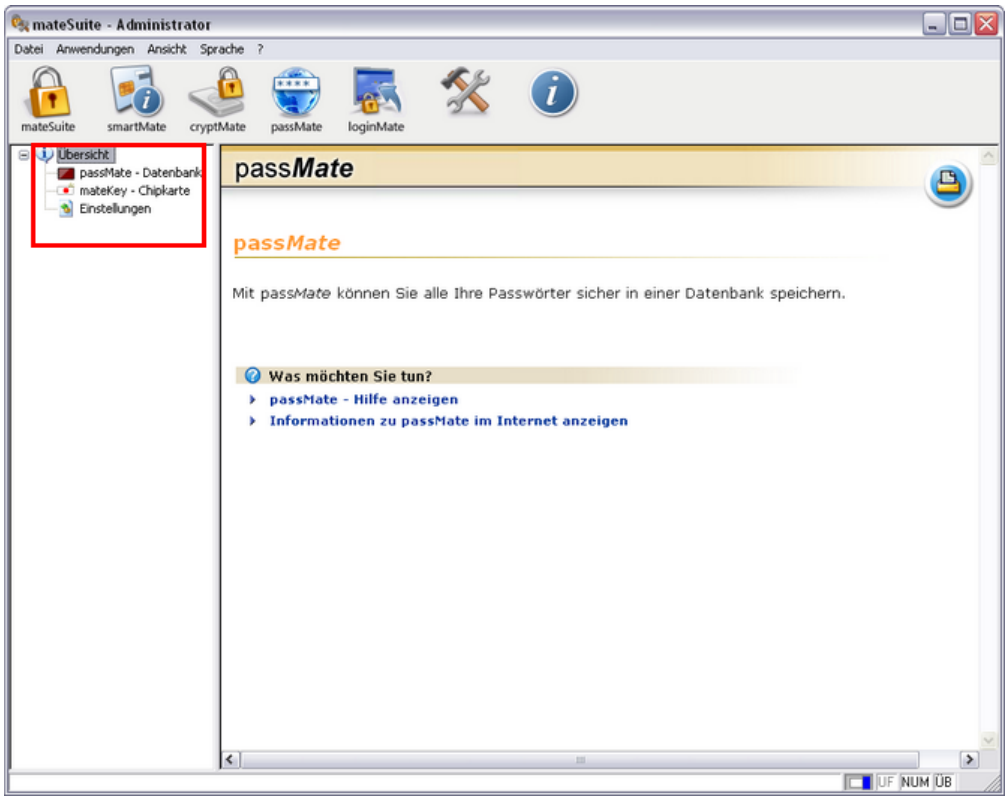
Wenn Sie den login***Mate***® Bildschirmschoner aktivieren, erscheint der login***Mate***® Bildschirmschoner bei Nichtbenutzung des PC's nach der vorgegebenen Zeit.

5.2.1.2 passMate

pass***Mate***® erleichtert die Verwaltung von Passwörtern und gewährleistet dabei eine hohe Sicherheit. Die sensiblen Passwortdaten werden in einer verschlüsselten Datei oder direkt auf der mateKey Security Card abgespeichert. Aus dieser Datenbank können Sie dann automatisch in die gewünschte Applikation oder der Eingabemaske des Browsers eingefügt werden.

Um mit passMate zu arbeiten, starten Sie mateSuite und klicken den Button passMate.

Es öffnet sich die Anwendung passMate. Auf der linken Seite befindet sich eine Baumstruktur, wo Sie die angelegte Datenbank oder die Datenbank auf der mateKey Karte auswählen können.

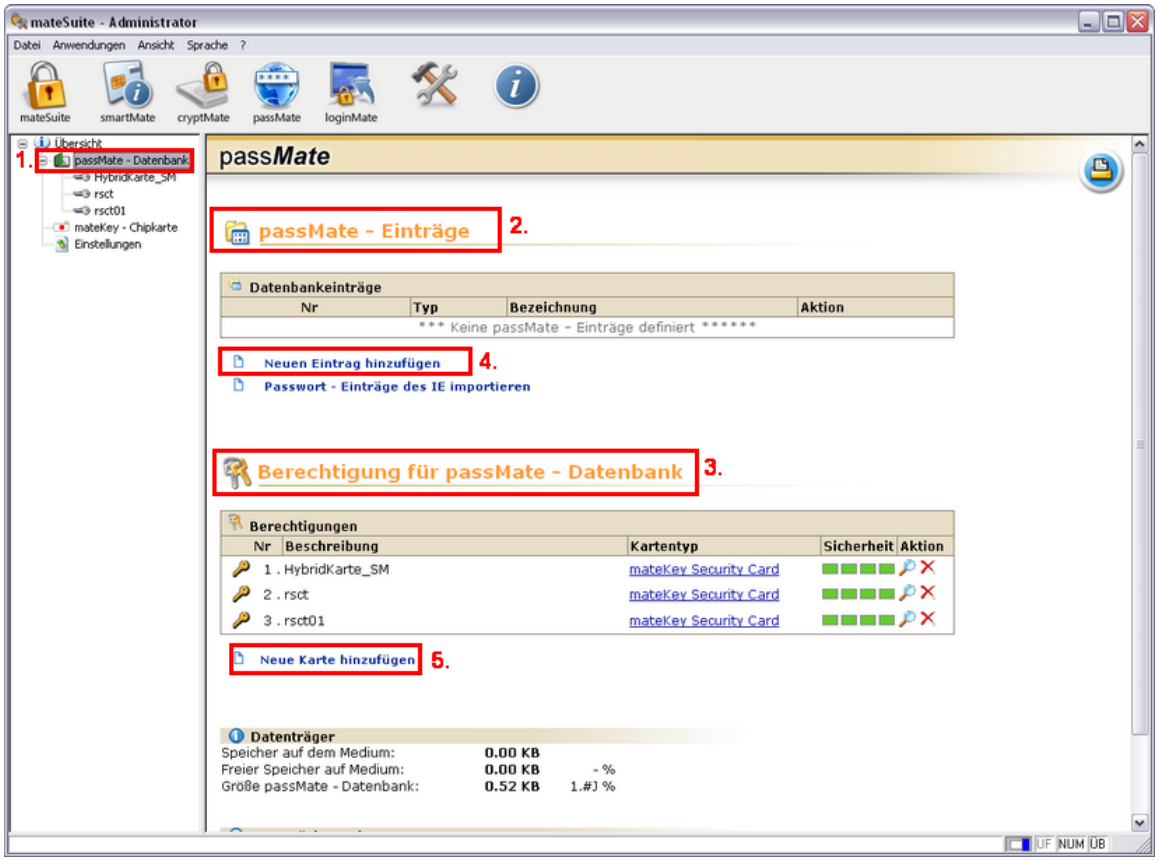


5.2.1.2.1 Passw orteinträge manuell anlegen

Um Passworteinträge anzulegen, muss erst eine Datenbank angelegt werden. Siehe hierzu: Schritt 5 Einrichtung passMate

pass***Mate***®-Einträge sind im Wesentlichen verschlüsselt abgelegte Tastaturmakros, die das automatische Ausfüllen von Passwortmasken ermöglichen. Zur Erfassung einfacher Makros steht ein Assistent zur Verfügung, für Masken mit einer größeren Anzahl auszufüllender Felder stehen bei Bedarf Steuerkommandos zur Verfügung, die alle Möglichkeiten bieten.

Öffnen Sie die Datenbank, indem Sie sie auf der linken Seite (1) auswählen. Sie sehen jetzt alle Information, die für diese Datenbank vorliegen. Sie sehen die Passworteinträge (2) und die vorhandenen Berechtigungen (3). Über Neue Karten hinzufügen können Sie weitere Berechtigungen hinzufügen. Der folgende Ablauf ist identisch mit dem Hinzufügen der Berechtigung im Einrichtungsassistenten im Schritt 5. Mit dem Kreuz ✕ können Sie vorhandene Berechtigungen wieder entfernen.

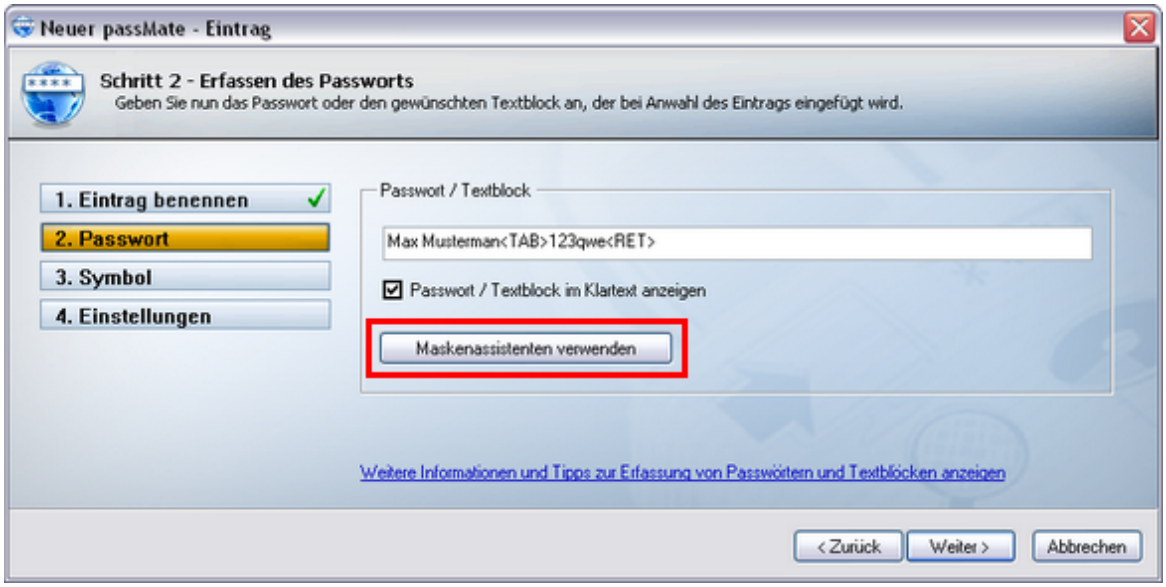


Um einen neuen Passworteintrag anzulegen, klicken Sie auf *Neuen Eintrag hinzufügen* (4)und folgen dem Einrichtungsassistenten.

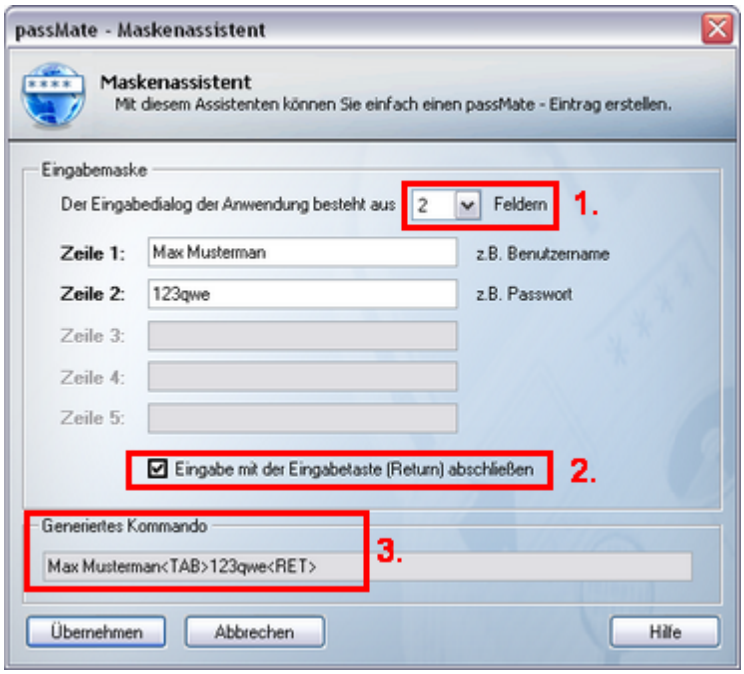
Schritt 1 - Eintrag benennen

Vergeben Sie hier einen sinnvollen Namen für den Passworteintrag.

Schritt 2 - Erfassen des Passworts


Neuer passMate - Eintrag
Schritt 2 - Erfassen des Passworts
Geben Sie nun das Passwort oder den gewünschten Textblock an, der bei Anwahl des Eintrags eingefügt wird.
1. Eintrag benennen
2. Passwort
3. Symbol
4. Einstellungen
Passwort / Textblock
Max Musterman<TAB>123qwe<RET>
Passwort / Textblock im Klartext anzeigen
Maskenassistenten verwenden
Weitere Informationen und Tipps zur Erfassung von Passwörtern und Textblöcken anzeigen
< Zurück
Weiter >
Abbrechen

Geben Sie Ihre Anmeldedaten ein. Beachten Sie dabei, dass Befehle wie <Return> oder <Tab> hier ebenso eingetragen werden müssen. Zu Ihrer Unterstützung verwenden Sie bitte den Maskenassistenten.



Geben Sie im Maskenassistenten die Anzahl der zu füllenden Felder (1) an. Füllen Sie die Felder mit Ihren Daten aus. Sollte der Eingabedialog mit der Eingabetaste abgeschlossen werden, setzen Sie entsprechend den Haken (2). Das generierte Kommando sehen Sie im Punkt (3).
Dieses Kommando können Sie gegebenenfalls noch ändern.

Zu weiteren Eingabe von Tastaturmakros stehen bei Bedarf folgende Kommandos zur Verfügung (bei der Eingabe Groß-/Kleinschreibung beachten):

- Return **<RET>**
- Tab **<TAB>**
- Shift + Tab **<BTAB>**
- Entfernen **<DEL>**
- Hoch **<UP>**

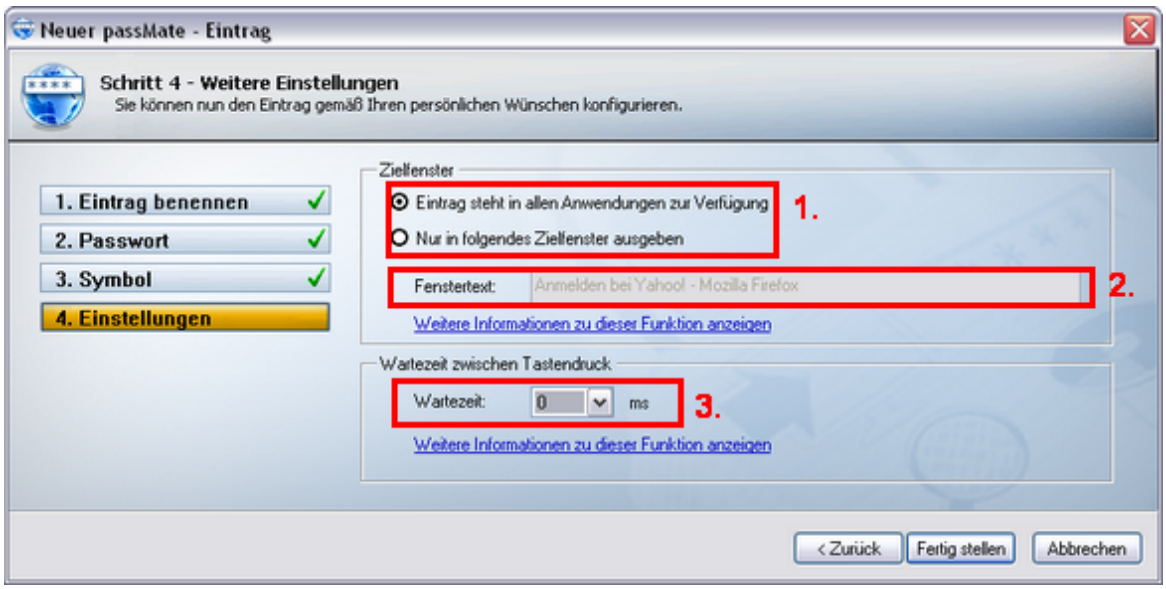
- Runter **<DOWN>**
- Links **<LEFT>**
- Rechts **<RIGHT>**
- Einfügen **<INS>**
- Zeilenanfang **<POS1>**
- Zeilenende **<END>**

Übernehmen Sie Ihre Eingaben und betätigen Sie den **Button Weiter**.

Schritt 3 - Zugeordnetes Symbol

Wählen Sie ein Symbol für diesen passMate-Eintrag aus.

Schritt 4 - Weitere Einstellungen



Im Schritt 4 der Einrichtung haben Sie die Möglichkeit auszuwählen (1), in welcher Anwendung der Passworteintrag zur Verfügung steht. Wenn Sie z.B. wollen, dass der Eintrag nur bei der Anmeldung an ein Yahoo - Konto verwendet werden kann, dann wählen Sie die entsprechende Option (1) aus. Als Fenstertext (2) geben Sie den Text an, der sich z.B. im Browser oben im Kopf befindet. In unserem Beispiel ist der Text "Anmelden bei Yahoo! - Mozilla Firefox". Um den Fenstertext automatisch auszufüllen, wechseln Sie in diesem Schritt in das gewünschte Fenster und wechseln dann zurück zu diesem Schritt. Der Text sollte nun als Fenstertext (2) zur Verfügung stehen.

Fenstertext im Browser

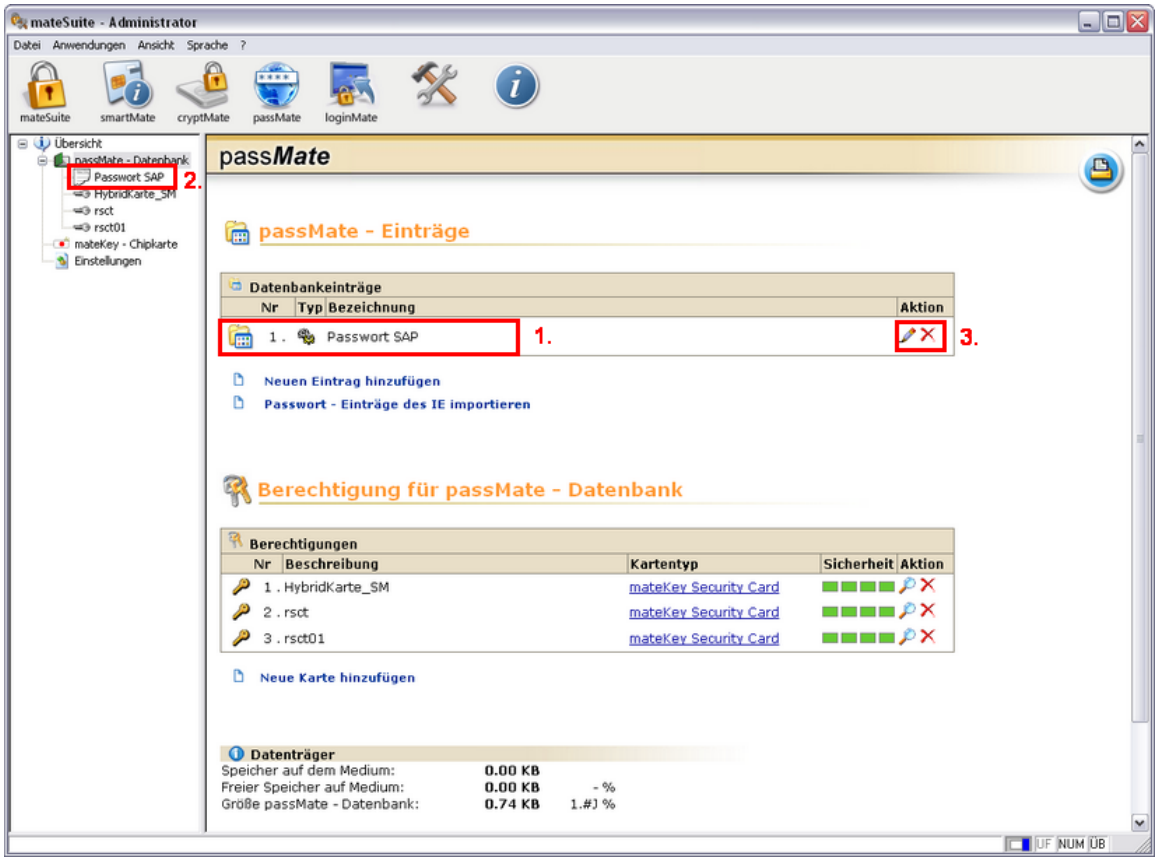
Dieser Passworteintrag kann nur ausgewählt werden, wenn Sie sich in diesem Fenster befinden.
Siehe hierzu auch: passMate Manager

Es kann vorkommen, dass in manchen Applikationen oder Browserfenstern die angelegten Passwörter nicht korrekt eingegeben werden. Hierzu erhöhen Sie die Wartezeit zwischen dem Tastendruck einfach (3). Da nicht vorausgesagt werden kann, welche Wartezeit optimal ist, erhöhen Sie die Wartezeit schrittweise, bis die Passwörter richtig eingegeben werden.
Bestätigen Sie Ihre Eingaben mit Fertig stellen und der Passworteintrag steht Ihnen zur Verfügung.

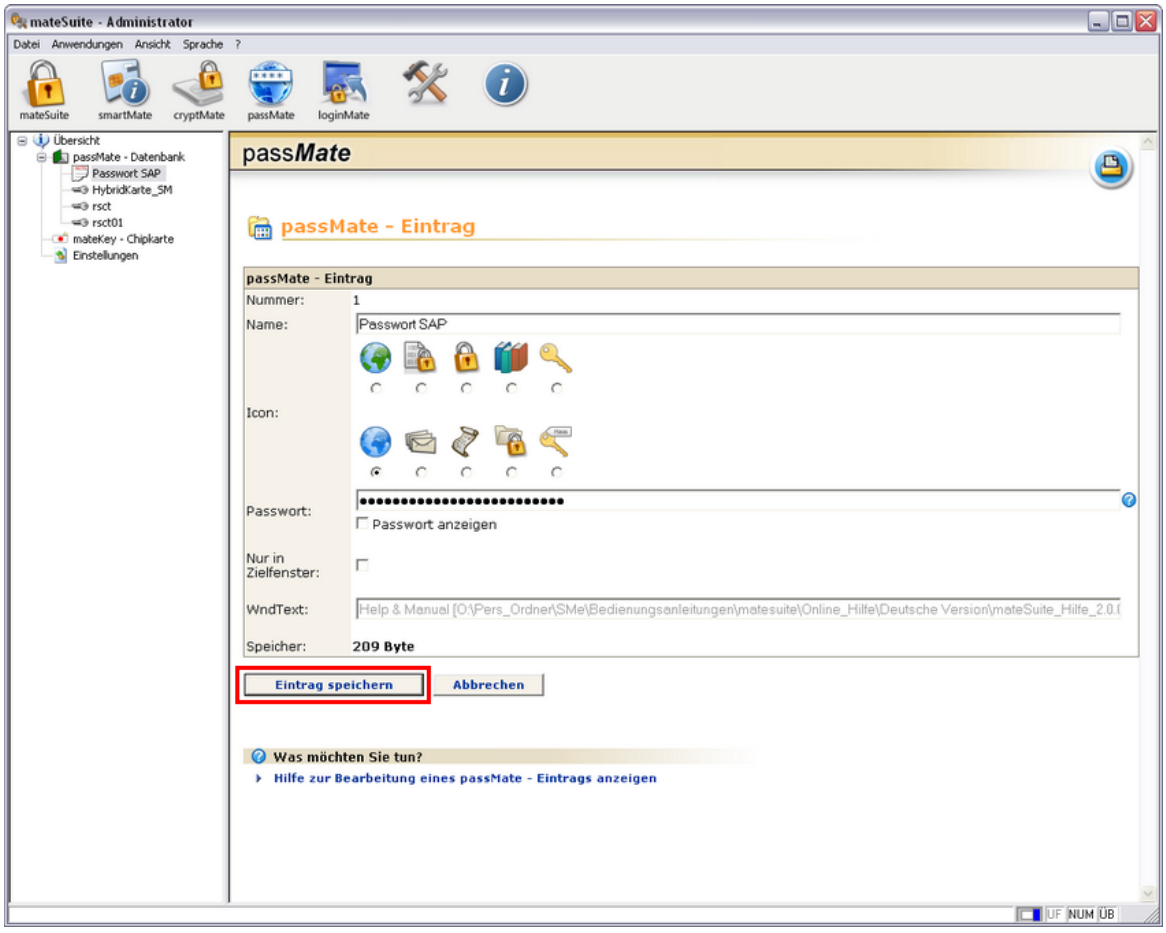
Siehe auch Internet Explorer-Plugin

5.2.1.2.2 Pasw orteinträge bearbeiten

Nachdem Sie den Passworteintrag erstellt haben, steht er Ihnen nun zur Verfügung (1).



Um Passworteinträge bearbeiten zu können, klicken Sie einfach auf den angelegten Passworteintrag (2) oder klicken Sie auf das Stiftsymbol (3). Das Kreuz löscht diesen Eintrag wieder.

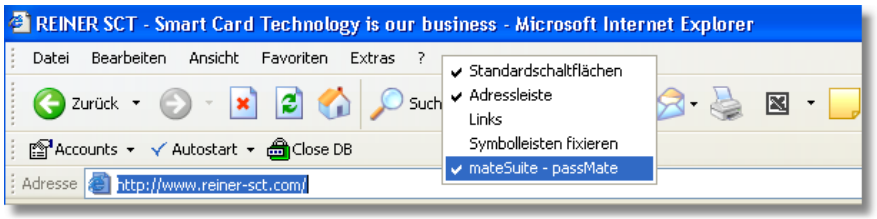


Sie haben nun die Möglichkeit verschiedene Änderungen vorzunehmen. Sie können den Namen, das Icon und das Passwort ändern. Um das Passwort zu ändern, müssen Sie zuerst den Haken bei *Passwort anzeigen* setzen, erst dann werden die Daten im Klartext dargestellt und können bearbeitet werden.
Außerdem können Sie noch die Wartezeit zwischen dem Tastendruck und das Zielfenster bearbeiten, in welchem der Passworteintrag ausgegeben werden soll. Bestätigen Sie Ihre Änderungen mit **Eintrag speichern**.

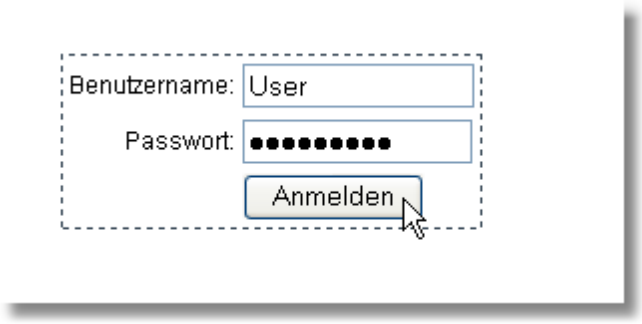
5.2.1.2.3 Internet Explorer-Plugin

Mit dem Internet Explorer-Plugin bietet passMate die Möglichkeit, die im Internet Explorer über die AutoVervollständigen-Funktion gespeicherten Passwörter, in die sichere pass***Mate***®-Datenbank zu importieren.

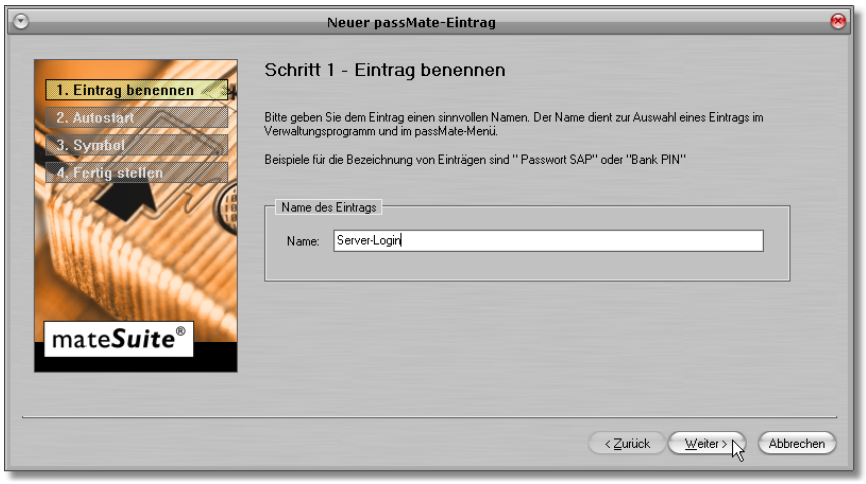
Das Plugin wird im Kontextmenü über die rechte Maustaste aktiviert und verfügt über die Buttons Accounts, Autostart und Open/Close DB.



Um Internet-Passwörter über das Plugin in pass***Mate*** zu speichern, wird das Passwort wie gewohnt in die Passwortmaske der Anwendung manuell eingegeben.

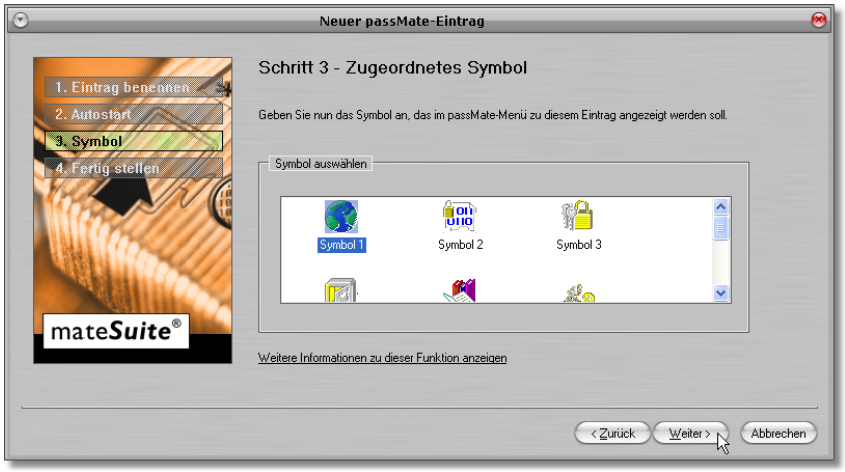


Handelt es sich um einen Standard-Passwortdialog, wird dies von pass***Mate***® erkannt und der folgende Assistent wird automatisch gestartet:


Neuer passMate-Eintrag
1. Eintrag benennen
2. Autostart
3. Symbol
4. Fertig stellen
mateSuite®
Schritt 1 - Eintrag benennen
Bitte geben Sie dem Eintrag einen sinnvollen Namen. Der Name dient zur Auswahl eines Eintrags im Verwaltungsprogramm und im passMate-Menü.
Beispiele für die Bezeichnung von Einträgen sind " Passwort SAP" oder "Bank PIN"
Name des Eintrags
Name:
Server-Login
< Zurück
Weiter >
Abbrechen

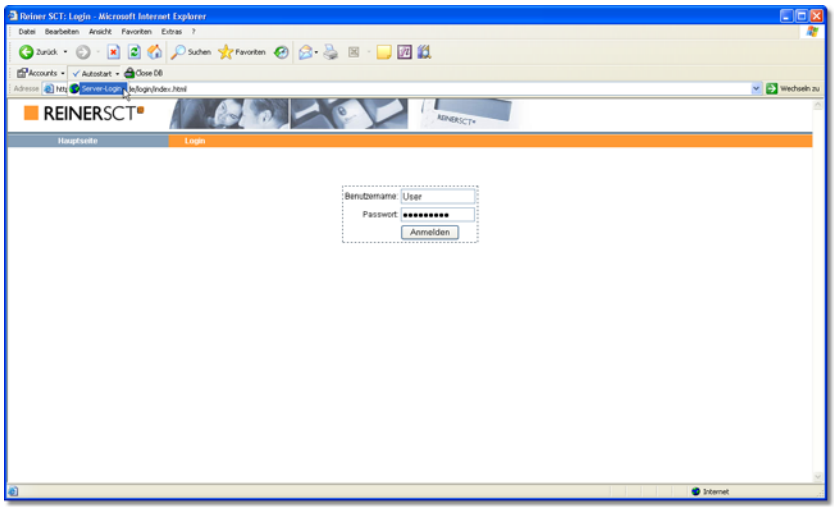
Im Schritt 1 wird der Name des Eintrags festgelegt, unter dem die Logindaten in pass***Mate***® verwaltet werden.

Im Schritt 2 wird festgelegt, ob die Autostart-Funktion verwendet werden soll. Ist diese aktiviert, wird der Link zum Aufruf der Passwortseite in der pass***Mate***® -Datenbank mit abgelegt. Ohne Autostart muss manuell auf die entsprechende Seite gegangen werden (z.B. über die Favoritenliste). Über den Button Accounts werden dann alle gültigen Logins für die besuchte Passwortmaske angezeigt und können ausgewählt werden.



Über das auszuwählende Symbol können Einträge gekennzeichnet werden. Nach dem Betätigen des Buttons <Fertig stellen> in der folgende Maske wird der Eintrag in die pass***Mate***-Datenbank eingetragen.

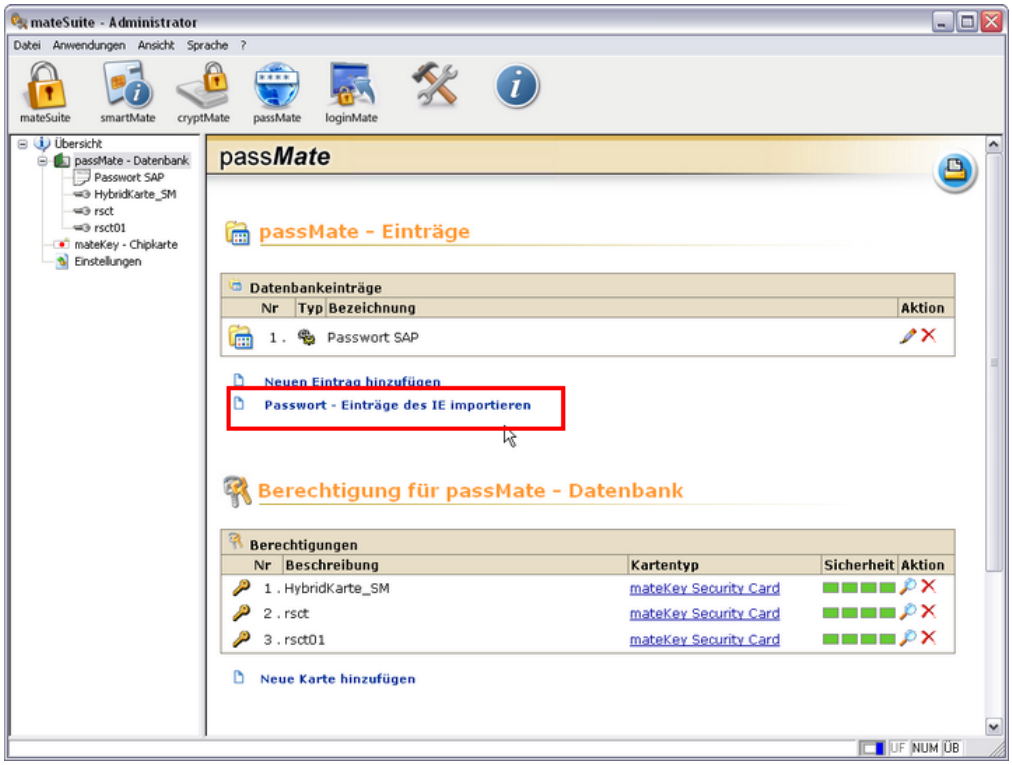
Über den Button Autostart kann nun die Seite aufgerufen und das Passwort in die Passwortmaske eingetragen werden.



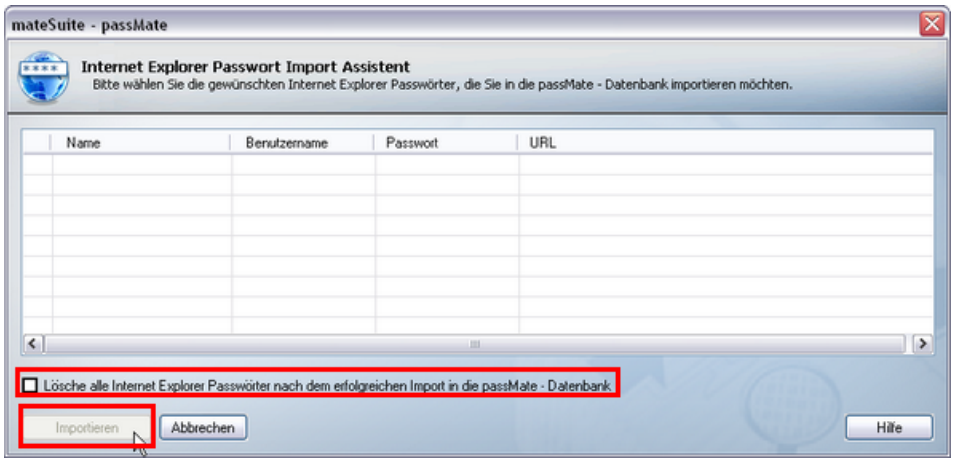
Passworteinträge, die über dieses Plugin erstellt wurden, können später nicht mehr bearbeitet werden.

Internet Explorer Passwort Import Assistent

Mit Hilfe des Internet Plugin haben Sie außerdem die Möglichkeit bereits gespeicherte Passwörter in die passMate Datenbank zu exportieren. Öffnen Sie die passMate Datenbank in der Anwendung passMate und klicken auf *Passwort Einträge des IE importieren*.



Es öffnet sich der IE Import Assistent, der alle gespeicherten Passwörter des Internet Explorers anzeigt. Über den Importieren Button werden alle Passwörter in die passMate Datenbank übernommen. Sie können auch diese Passwörter während des Importes aus dem Internet Explorer löschen, so dass sie sicher in der passMate Datenbank liegen. Setzen Sie dafür den Haken bei *Löschen aller Internet Explorer Passwörter nach*....

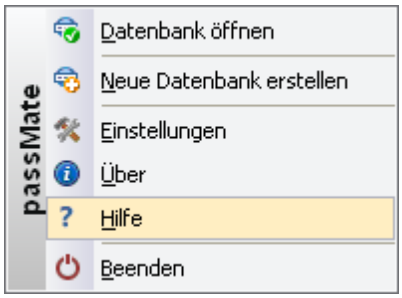

mateSuite - passMate
Internet Explorer Passwort Import Assistent
Bitte wählen Sie die gewünschten Internet Explorer Passwörter, die Sie in die passMate - Datenbank importieren möchten.
Name
Benutzername
Passwort
URL
Lösche alle Internet Explorer Passwörter nach dem erfolgreichen Import in die passMate - Datenbank
Importieren
Abbrechen
Hilfe

5.2.1.2.4 passMate-Manager

Der pass***Mate***® Manager erlaubt eine einfache und schnelle Verwaltung von Datenbanken und Passwörtern. Der Zugriff auf Anmeldedaten erfolgt mit dem pass***Mate***® Manager unkompliziert und vor allem sicher.

Durch die Voreinstellungen von mate***Suite*** wird pass***Mate***® automatisch beim Systemstart geladen. Vom Infobereich der Taskleiste, können Sie den pass***Mate***® Manager starten. Klicken Sie mit der rechten Maustaste auf folgendes Symbol:

Über das Menü können Sie alle Funktionen von pass***Mate***® nutzen, ohne den mate***Suite***-Administrator zu starten. Es stehen folgende Funktionen zur Verfügung:



Datenbank öffnen

Öffnet die bereits erstellte Datenbank.
Sie können auch eine Datenbank öffnen, indem Sie einfach auf das Symbol mit der linken Maustaste klicken. Das passMate Manager Symbol verändert sich und die Datenbank ist aktiv.

Datenbank geschlossen

Datenbank geöffnet

Neue Datenbank erstellen

Hier können Sie eine neue Datenbank erstellen. Der folgende Ablauf ist identisch mit der Einrichtung im Einrichtungsassistenten im Schritt 5.

Einstellungen

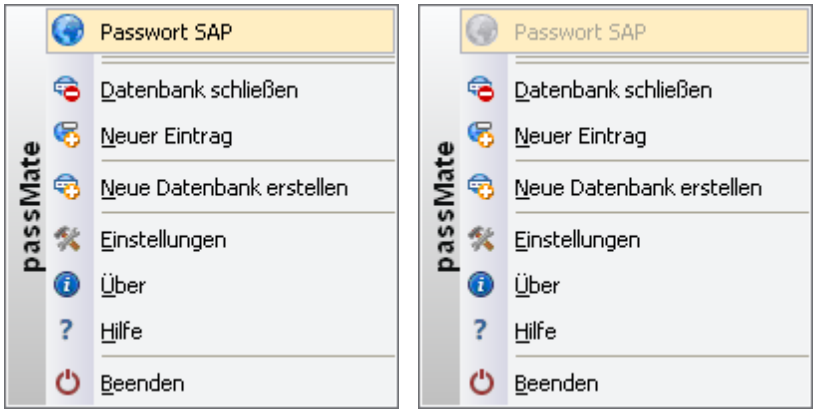
Öffnet den mate***Suite***-Administrator unter der Anwendung passMate. Hier können neue Datenbanken erfasst und verwaltet werden.

Ist die Datenbank geöffnet, stehen noch folgende Funktionen bereit.

Zugangsdaten auswählen

Gespeicherte Passworteinträge sind im pass***Mate***®-Manager gelistet und können dort nach Bedarf ausgewählt werden.

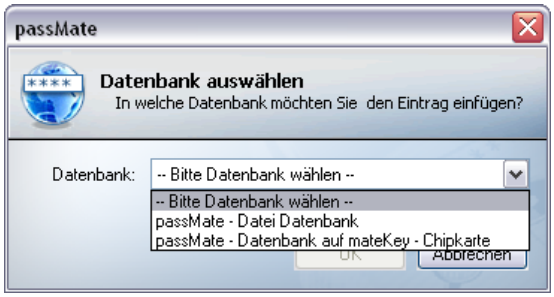
Wurde beim Anlegen des Passworteintrages die Option *Nur in folgendes Zielfenster ausgeben* gewählt, so wird der Datenbankeintrag erst aktiviert, wenn das betreffende Eingabefenster auch tatsächlich aktiv ist. So wird vermieden, dass Zugangsdaten versehentlich in falsche Masken ausgegeben werden.



Aktiver Eintrag **Inaktiver Eintrag**

Neuer Eintrag

Sie können einen neuen Passworteintrag erstellen. Wählen Sie zuerst, ob der Eintrag auf der mateKey - Chipkarte oder in der Datei Datenbank gespeichert werden soll.

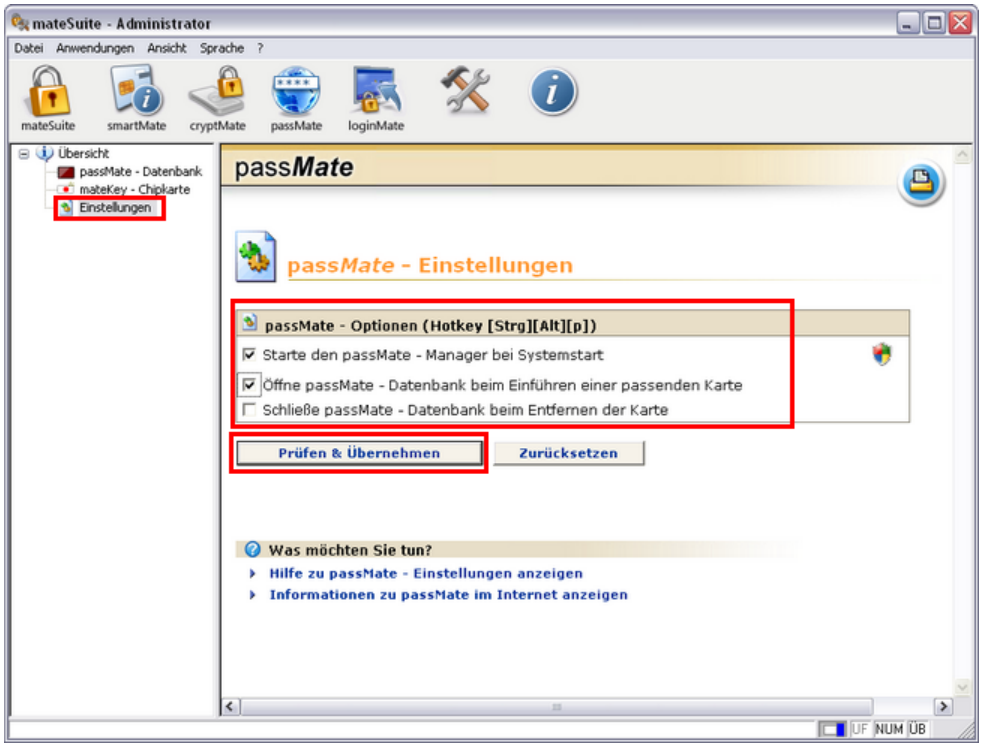


Wählen Sie die entsprechende Option aus und Sie können einen neuen Eintrag erstellen, der Ihnen dann zur Verfügung steht.

5.2.1.2.5 Einstellungen

Klicken Sie bei pass***Mate***® links auf Einstellungen und Sie können folgende Optionen einstellen.

Starte den passMate-Manager bei Systemstart
Öffne passMate - Datenbank beim Einführen einer passenden Karte: Die Datenbank wird automatisch geöffnet, sobald eine passende Karte in den Kartenleser gesteckt wird.
Schließe passMate - Datenbank beim Entfernen der Karte: Die Datenbank wird automatisch geschlossen, sobald die Karte wieder gezogen wird.



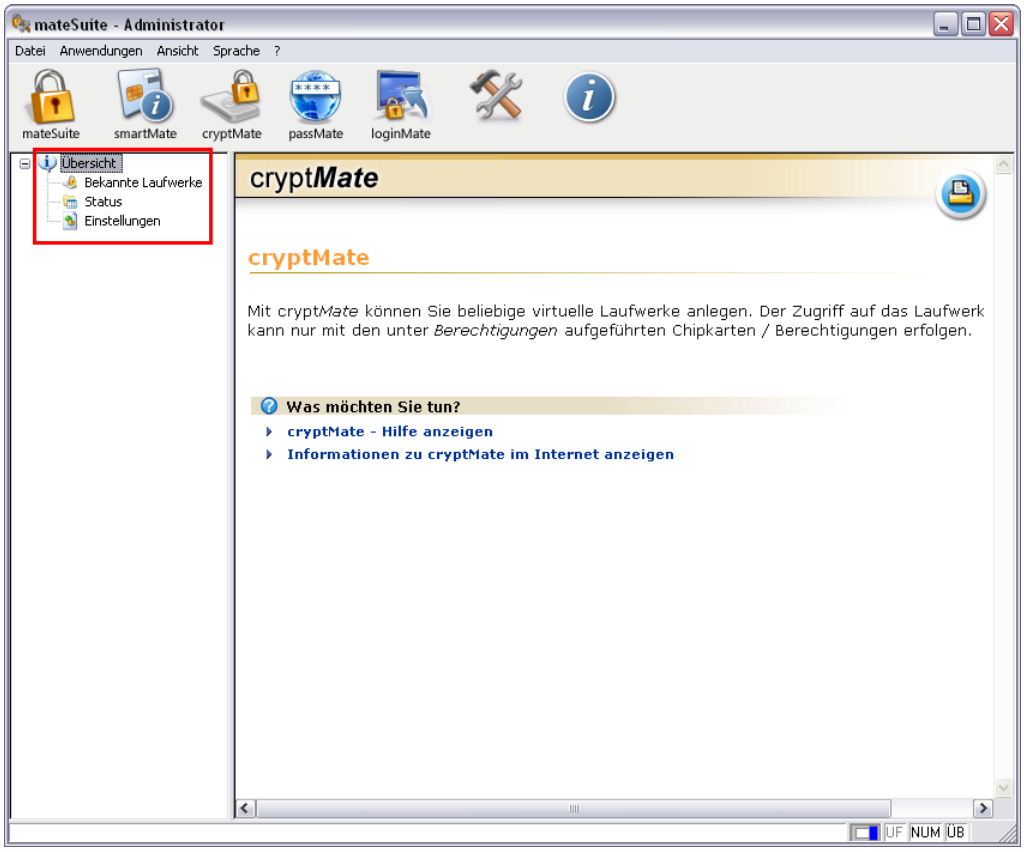
Bestätigen Sie Ihre Auswahl mit **Prüfen & Übernehmen.**

5.2.1.3 cryptMate

Mit crypt***Mate***® können auf Datenträgern (Festplatten, USB-Sticks, Internet-Laufwerken etc.) virtuelle verschlüsselte Laufwerke eingerichtet werden. Diese Laufwerke werden mittels Chipkarte verschlüsselt. Das Laufwerk wird erst freigeschaltet, wenn die entsprechende Karte in den Chipkartenleser eingeführt wird.

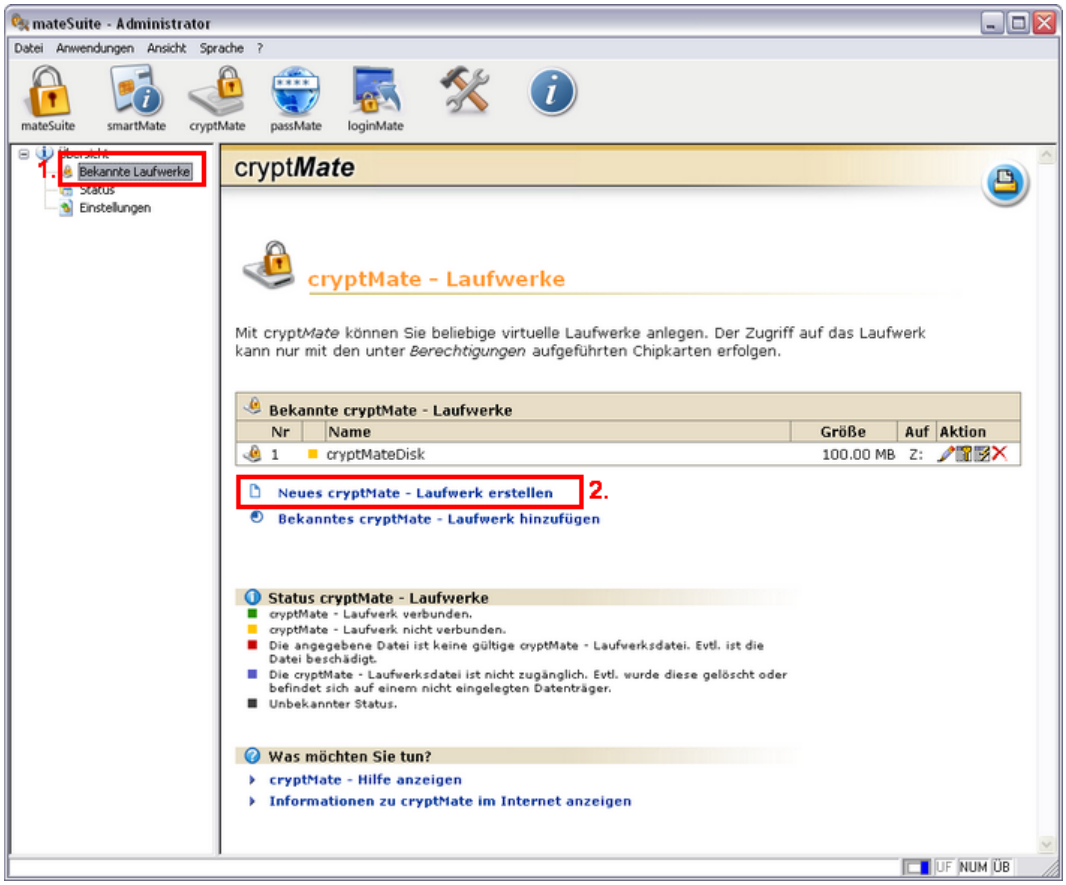
Um mit cryptMate zu arbeiten, starten Sie mateSuite und klicken den Button cryptMate.

Es öffnet sich die Anwendung cryptMate. Auf der linken Seite können Sie sich bereits angelegte cryptMate Laufwerke über *Bekannte Laufwerke* anzeigen lassen. Über *Status* können Sie sich die aktuelle Laufwerkssituation Ihres Systems anzeigen lassen.

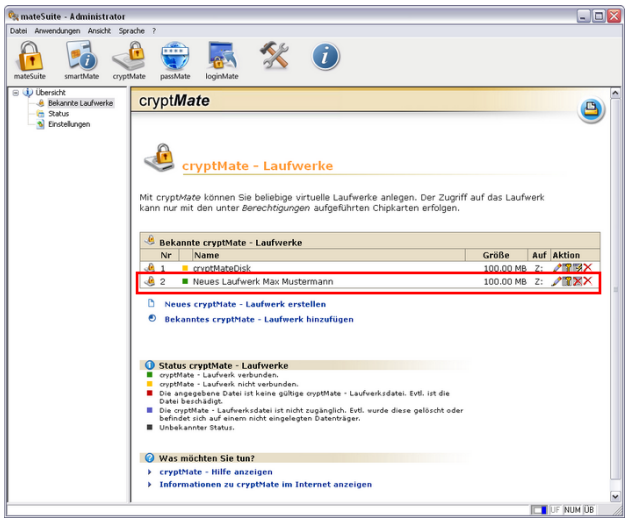


5.2.1.3.1 Virtuelles Laufwerk erstellen und verschlüsseln

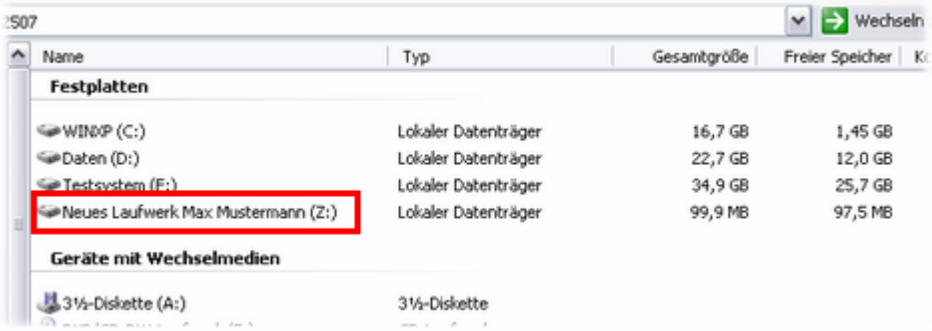
Um ein cryptmate Laufwerk zu erstellen, klicken Sie auf *Bekannte Laufwerke* (1) und dann auf *Neues cryptMate - Laufwerk erstellen* (2).



Der folgende Ablauf ist identisch mit der Einrichtung im Einrichtungsassistenten im Schritt 6.


mateSuite - Administrator
cryptMate
cryptMate - Laufwerke
Bekannte cryptMate - Laufwerke
1 cryptMateDisk 100.00 MB Z:
2 Neues Laufwerk Max Mustermann 100.00 MB Z:
Neues cryptMate - Laufwerk erstellen
Bekanntes cryptMate - Laufwerk hinzufügen
Status cryptMate - Laufwerke
Was möchten Sie tun?
cryptMate - Hilfe anzeigen
Informationen zu cryptMate im Internet anzeigen

Nach erfolgreichem Abschluss der Assistenten erscheint das Laufwerk in der Liste der bekannten Laufwerke.
Nach dem das angelegte crypt***Mate***®-Laufwerk verbunden wurde, erscheint es innerhalb des Windows-Betriebssystems unter dem definierten Laufwerksbuchstaben und der Volume-Bezeichnung.



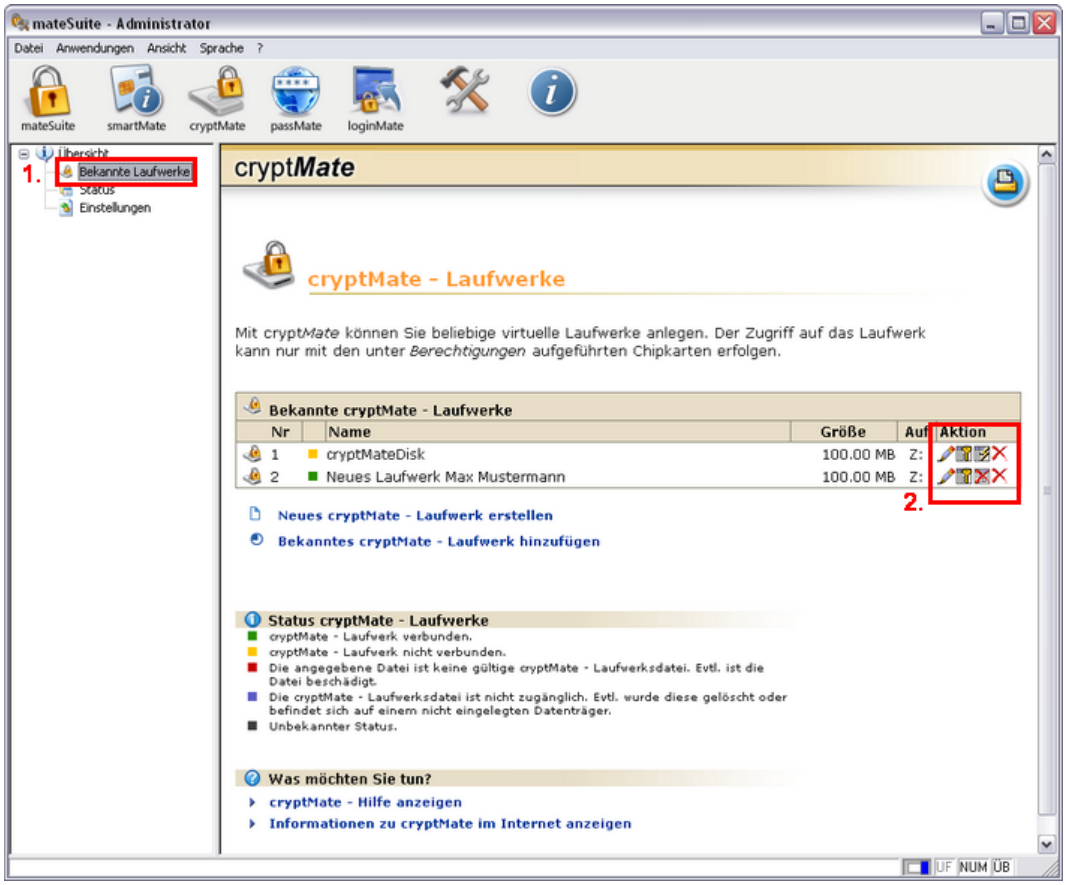
5.2.1.3.2 Verwaltung von virtuellen Laufwerken

Die crypt***Mate***®-Laufwerksverwaltung bietet folgende Funktionen:

- crypt***Mate***®-Laufwerke anzeigen
- Neue crypt***Mate***®-Laufwerke erstellen
- crypt***Mate***®-Laufwerke löschen
- Bekannte crypt***Mate***®-Laufwerke hinzufügen
- Berechtigungen zu crypt***Mate***®-Laufwerken vergeben bzw. löschen
- Einstellungen zu crypt***Mate***®-Laufwerken vornehmen

Ansicht bekannter Laufwerke

Wenn Sie links auf *Bekannte Laufwerke* (1) klicken, sehen Sie welche Laufwerke Sie eingerichtet haben.


mateSuite - Administrator
Datei Anwendungen Ansicht Sprache ?
mateSuite
smartMate
cryptMate
passMate
loginMate
Übersicht
1.
Bekannte Laufwerke
Status
Einstellungen
cryptMate
cryptMate - Laufwerke
Mit cryptMate können Sie beliebige virtuelle Laufwerke anlegen. Der Zugriff auf das Laufwerk kann nur mit den unter Berechtigungen aufgeführten Chipkarten erfolgen.
Bekannte cryptMate - Laufwerke
Nr
Name
Größe
Auf
Aktion
1
cryptMateDisk
100.00 MB
Z:
2
Neues Laufwerk Max Mustermann
100.00 MB
Z:
2.
Neues cryptMate - Laufwerk erstellen
Bekanntes cryptMate - Laufwerk hinzufügen
Status cryptMate - Laufwerke
cryptMate - Laufwerk verbunden.
cryptMate - Laufwerk nicht verbunden.
Die angegebene Datei ist keine gültige cryptMate - Laufwerksdatei. Evtl. ist die Datei beschädigt.
Die cryptMate - Laufwerksdatei ist nicht zugänglich. Evtl. wurde diese gelöscht oder befindet sich auf einem nicht eingelegten Datenträger.
Unbekannter Status.
Was möchten Sie tun?
cryptMate - Hilfe anzeigen
Informationen zu cryptMate im Internet anzeigen
UF NUM ÜB

cryptMate®-Laufwerk bearbeiten

Klicken Sie auf den **Stift** (2), um das Laufwerk zu bearbeiten.

Hier können Sie folgende Einstellungen vornehmen.
Name: Hier können Sie den Namen des virtuellen Laufwerks ändern.
Control Datei: Hier können Sie dem virtuellen Laufwerk eine andere Laufwerksdatei zuordnen.
Schreibgeschützt verbinden: Die Option bewirkt, dass das Laufwerk schreibgeschützt verbunden wird. Sie haben dann nur Leserechte.
Als Wechselplatte verbinden: Das Laufwerk wird von Windows wie eine Wechselplatte behandelt, d.h. systeminterne Ordner oder Dateien, wie z.B. Wiederherstellungspunkte, Sicherungen oder der Papierkorbordner werden auf diesem Laufwerk nicht erstellt.
Mount Manager benachrichtigen: Die Datenträgerverwaltung von Windows überwacht das Verbinden der Festplatte und kann so die Verwaltung des Datenträgers überwachen. Es wird empfohlen den Haken zu setzen.

Bestätigen Sie Ihre Änderungen mit dem **Button Eintrag speichern** (3).

Mit dem Kreuz (2) können Sie vorhandene Laufwerke löschen.

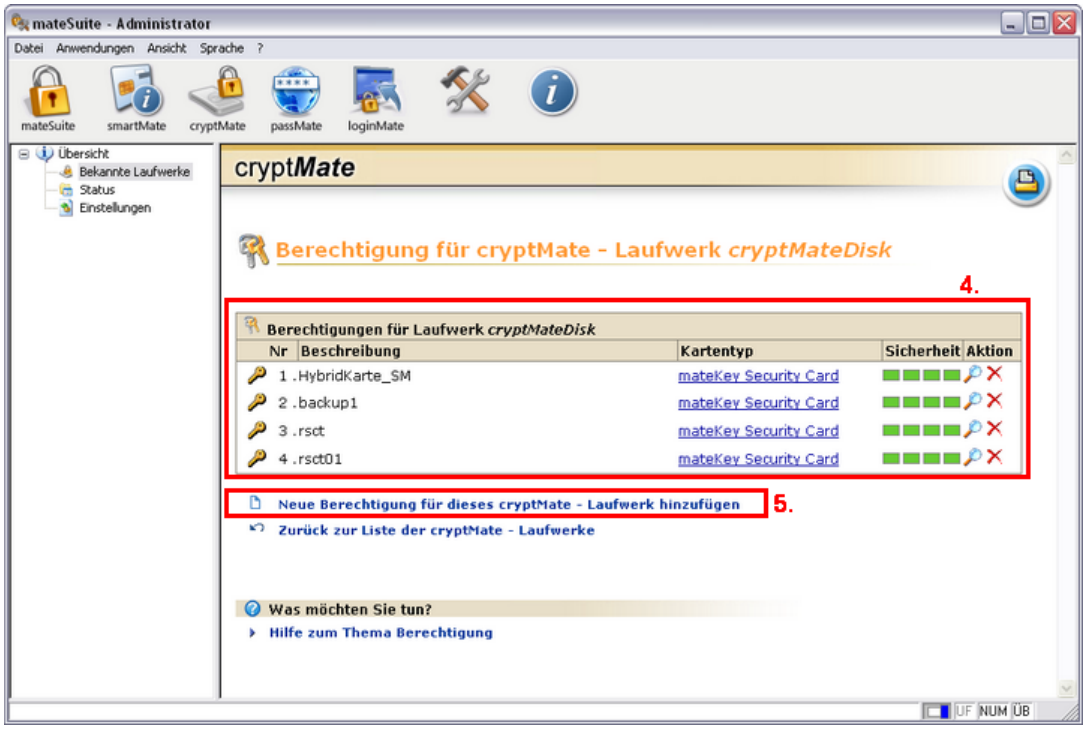
Verbinden und trennen von Laufwerken

Verbindet ein Laufwerk

Trennt ein Laufwerk

Berechtigungen vergeben/löschen

Um Berechtigungen für die Laufwerke hinzuzufügen, klicken Sie auf das -Symbol (2). Das Laufwerk muss vorher getrennt sein.



Sie sehen hier alle zu diesem Laufwerk vorhandenen Berechtigungen (4). Um weitere Berechtigungen hinzuzufügen, klicken Sie *Eine neue Berechtigung zu diesem cryptMate - Laufwerk hinzufügen* (5). Der folgende Ablauf ist identisch mit dem Hinzufügen der Berechtigung im Einrichtungsassistenten im Schritt 6. Mit dem Kreuz ✕ können Sie vorhandene Berechtigungen wieder entfernen.

5.2.1.3.3 cryptMate-Manager

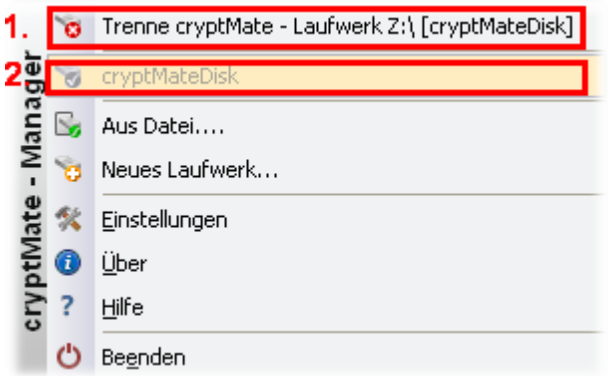
Der crypt***Mate***® Manager erlaubt eine einfache und schnelle Verwaltung von virtuellen Laufwerken. Sie können neue Laufwerke erstellen, aktivieren oder deaktivieren.

Durch die Voreinstellungen von mate***Suite*** wird crypt***Mate***® automatisch beim Systemstart geladen. Vom Infobereich der Taskleiste aus, können Sie den crypt***Mate***® Manager starten. Klicken Sie mit der rechten Maustaste auf dieses Symbol:

Laufwerk verbunden

Laufwerk getrennt

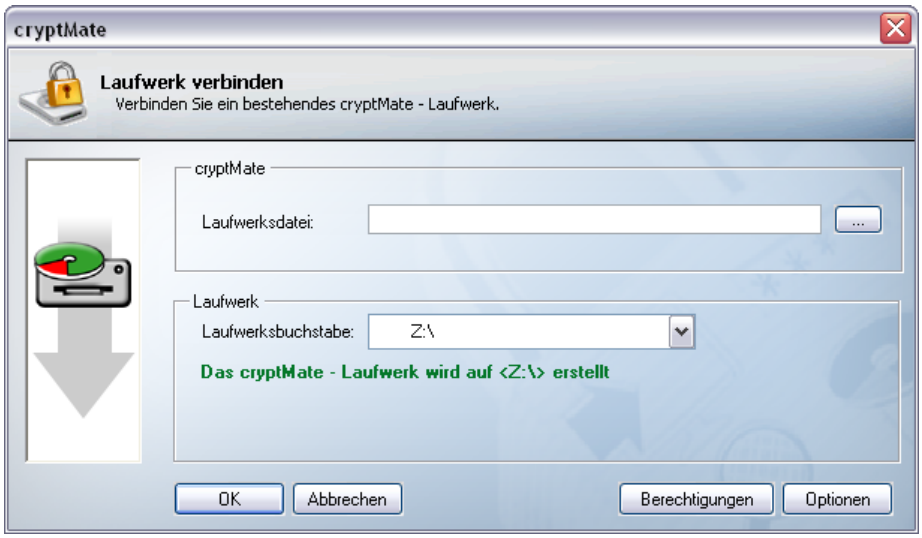
Über das Kontextmenü können Sie alle Funktionen von crypt***Mate***® nutzen, ohne den mate***Suite*** Administrator zu starten. Es stehen folgende Funktionen zur Verfügung:



Laufwerke trennen
Mit linkem Mausklick können die verbundenen Laufwerke getrennt werden (1).

Laufwerke verbinden
Mit linkem Mausklick wird das virtuelle Laufwerk wieder verbunden (2). Das Laufwerk ist freigeschaltet und wird unter dem Arbeitsplatz als lokales Laufwerk aufgeführt.

Aus Datei
Mit linkem Mausklick können crypt***Mate***®-Laufwerksdateien aufgerufen werden, sofern sie noch keinem Laufwerk zugeordnet sind und zu einem virtuellen Laufwerk umgewandelt werden.



Suchen Sie eine vorhanden Laufwerksdatei aus. Bestimmen Sie den Laufwerksbuchstaben des virtuellen Laufwerkes und bestätigen mit dem **Button OK**. Sie können noch ggf. Berechtigungen und Optionen auswählen.

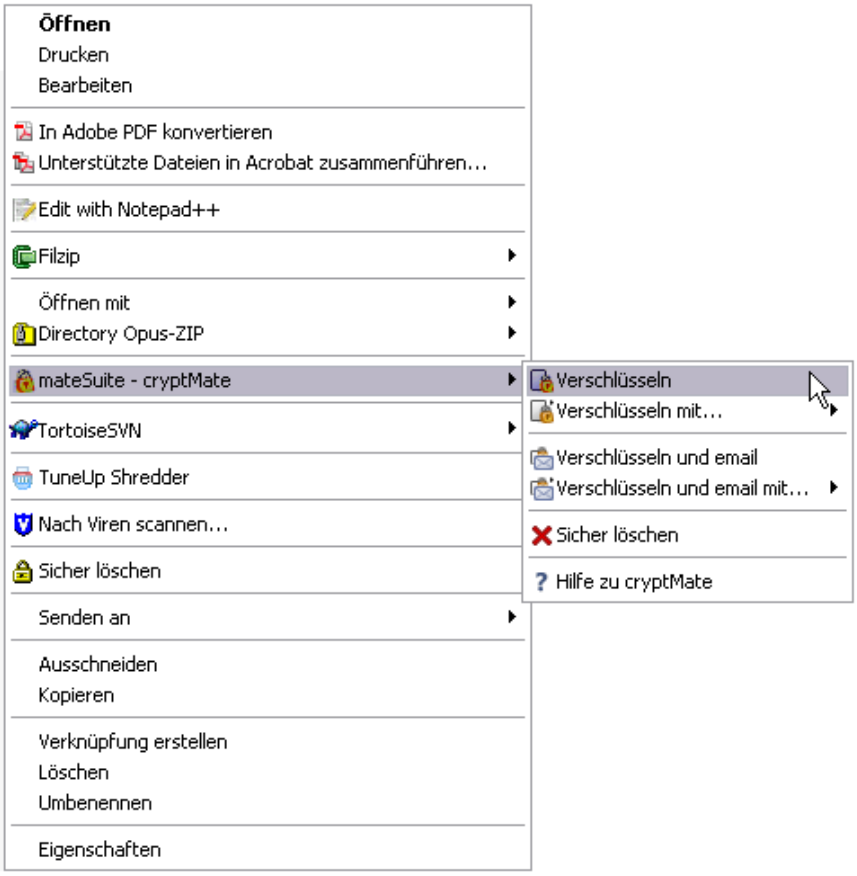
Neues Laufwerk
Startet den Einrichtungsassistenten, um ein neues Laufwerk zu erstellen und zu verschlüsseln.

5.2.1.3.4 Einstellungen

In den Einstellungen zu crypt***Mate***® lässt sich einstellen, ob der crypt***Mate***®-Manager automatisch bei Systemstart gestartet werden soll.

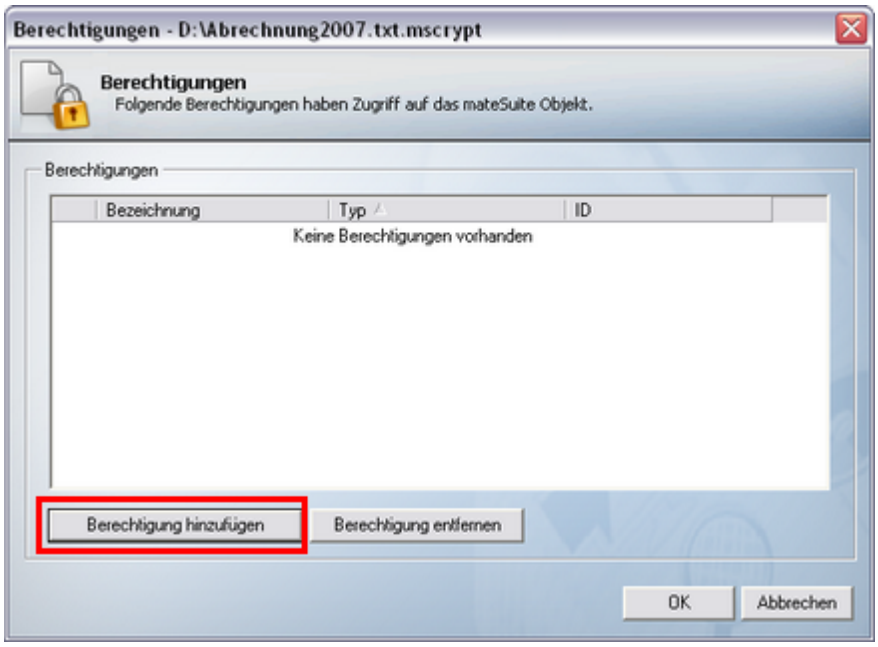
5.2.1.3.5 Verschlüsseln von Dateien und Ordner

Mit cryptMate haben Sie die Möglichkeit im Kontextmenü des Explorer, Dateien und ganze Ordner zu verschlüsseln und per E-Mail zu verschicken. Die Verschlüsselung, die cryptMate verwendet, basiert auf eine Asymmetrische Verschlüsselung. Detaillierte Informationen zum Thema Asymmetrische Verschlüsselung finden Sie hier.
Um eine Datei oder einen Ordner zu verschlüsseln, klicken Sie im Explorer mit der rechten Maustaste auf die Datei oder den Ordner und folgendes Kontextmenü öffnet sich.



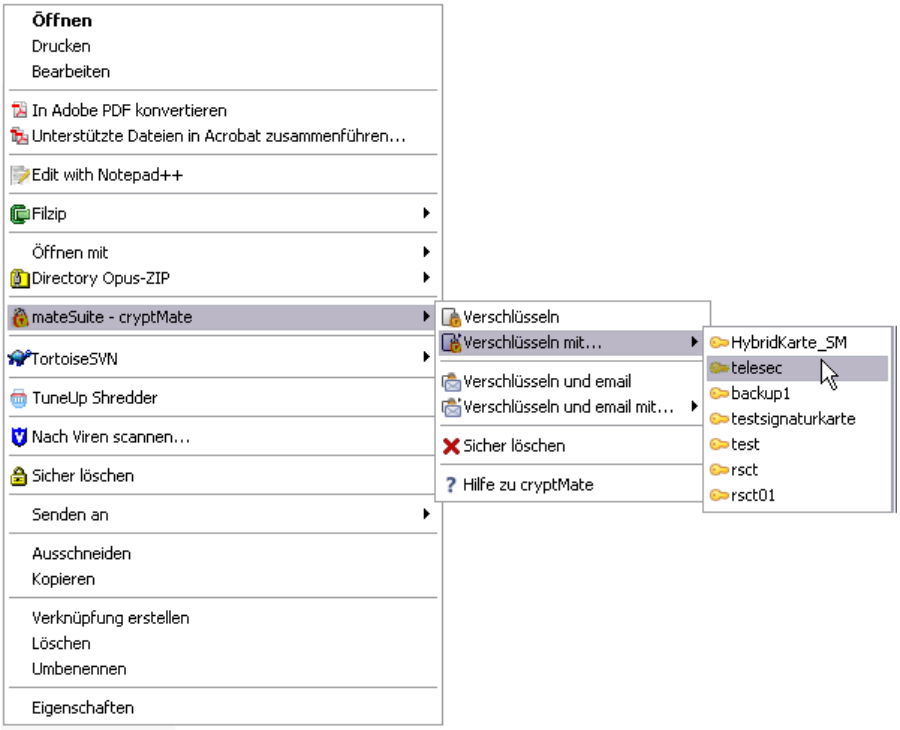
Verschlüsseln

Wählen Sie *Verschlüsseln* und es öffnet sich folgender Assistent.



Hier fügen Sie die Berechtigungen hinzu, mit denen dann später die Datei oder der Ordner wieder entschlüsselt werden kann. Nach Beendigung der Verschlüsselung erhalten Sie eine Datei mit der Endung *.mscrypt.

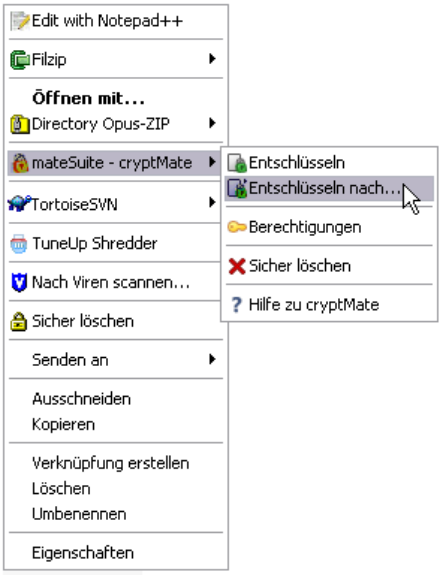
Wenn Sie *Verschlüsseln mit* wählen, können Sie berechtigte Karten, die schon angelegt wurden, direkt aus dem Kontextmenü wählen. Diese bekannten Berechtigungen sind öffentliche Schlüssel, die aus den Karten generiert wurden.



Die bekannten Berechtigungen, die Sie hier verwenden, sind nur mit Chipkarten, die einem RSA Algorithmus verwenden, möglich. Informationen zu den verschiedenen Karten erhalten Sie in der Software unter ? -> Bekannte Karten.

Entschlüsseln/ Entschlüsseln nach

Die verschlüsselte Datei kann weder geöffnet noch bearbeitet werden. Nur mit Hilfe von cryptMate und der berechtigten, physisch vorhandenen Karte kann die Datei oder der Ordner wieder entschlüsselt werden. Klicken Sie mit der rechten Maustaste auf die verschlüsselte Datei. Wenn Sie *Entschlüsseln* wählen, wird die Datei in dem gleichen Verzeichnis entschlüsselt. Wenn Sie *Entschlüsseln nach* wählen, können Sie das Verzeichnis auswählen, in dem die Datei entschlüsselt werden soll.



Verschlüsseln und email/ mit...

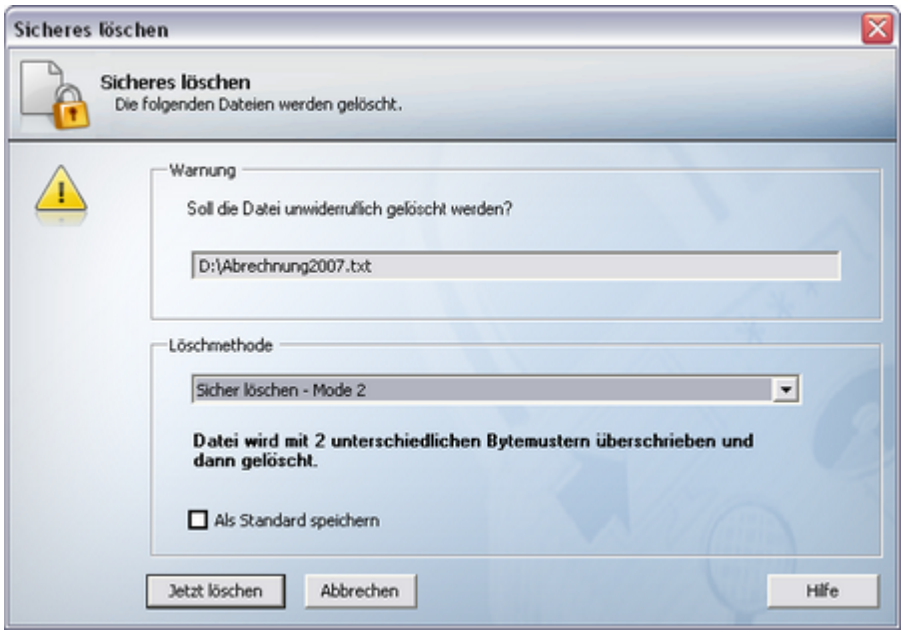
Sie können die Daten verschlüsseln und gleich per email verschicken.

Voraussetzungen dafür sind:
1. Der Empfänger und der Sender der E-Mail besitzen mateSuite bzw. cryptMate.
2. Sie als Sender müssen den öffentlichen Schlüssel/ Berechtigung des Empfängers haben, um die Datei zu verschlüsseln, so dass der Empfänger der E-Mail sie mit seinem privaten Schlüssel (physisch vorhandene Karte) entschlüsseln kann. Dies ist das Prinzip der asymmetrischen Verschlüsselung.

Sie als Sender benötigen deshalb einmalig eine RSA Chipkarte des Empfängers, um diese als öffentlichen Schlüssel/ Berechtigung anzulegen. Wenn Sie die Daten mit der entsprechenden Berechtigung verschlüsselt haben, öffnet sich automatisch Ihr Standard E-Mail Programm (z.B. Outlook) und Sie können die verschlüsselten Daten versenden.

Sicher löschen

Mit der Funktion **Sicher löschen** stehen Ihnen fünf verschiedene Löschmethoden zur Verfügung, um Ihre Daten sicher und unwiderruflich zu löschen.



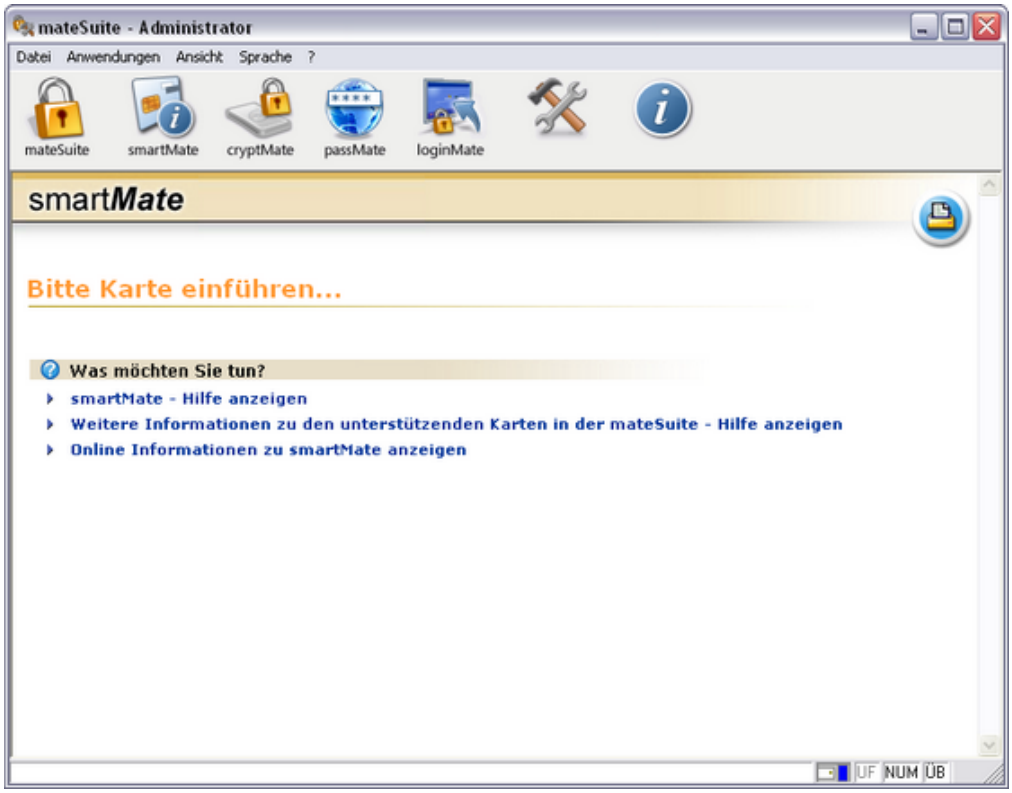
Wenn Sie über die Windowsfunktion Löschen gehen, würden die Daten erst in den Papierkorb verschoben und wenn Sie den Papierkorb leeren, können die Daten immer noch mit entsprechenden Programmen wiederhergestellt werden. Um dies zu verhindern, verwenden Sie eine der Methoden **Sicher löschen Mode 1-4**.
Die Methode **Nur löschen** bedeutet das Gleiche, als wenn Sie Shift + Entf drücken würden. Die Daten werden gelöscht, ohne dass sie in den Papierkorb verschoben werden.

Sicher löschen - Mode 1 überschreibt die zu löschenden Daten zuerst mit Nullen und wird dann gelöscht.
Sicher löschen - Mode 2 überschreibt die zu löschenden Daten zuerst mit 2 unterschiedlichen Bytemustern und wird dann gelöscht.
Sicher löschen - Mode 3 überschreibt die zu löschenden Daten zuerst mit 4 unterschiedlichen Bytemustern und wird dann gelöscht.
Sicher löschen - Mode 4 überschreibt die zu löschenden Daten zuerst mit 8 unterschiedlichen Bytemustern und wird dann gelöscht.

Die sicherste Methode ist Mode 4. Aber diese Löschaktion dauert auch am längsten. Wenn Sie also große Dateien oder Ordner sicher löschen wollen, kann dies einige Zeit in Anspruch nehmen.

5.2.1.4 smartMate

Mit smart***Mate***® lassen sich Informationen zu den von mate***Suite*** unterstützten Chipkarten auslesen. Je nach Kartentyp sind der Umgang der Informationen und die Bearbeitungsmöglichkeiten sehr unterschiedlich. Alle Informationen lassen sich auch ausdrucken.



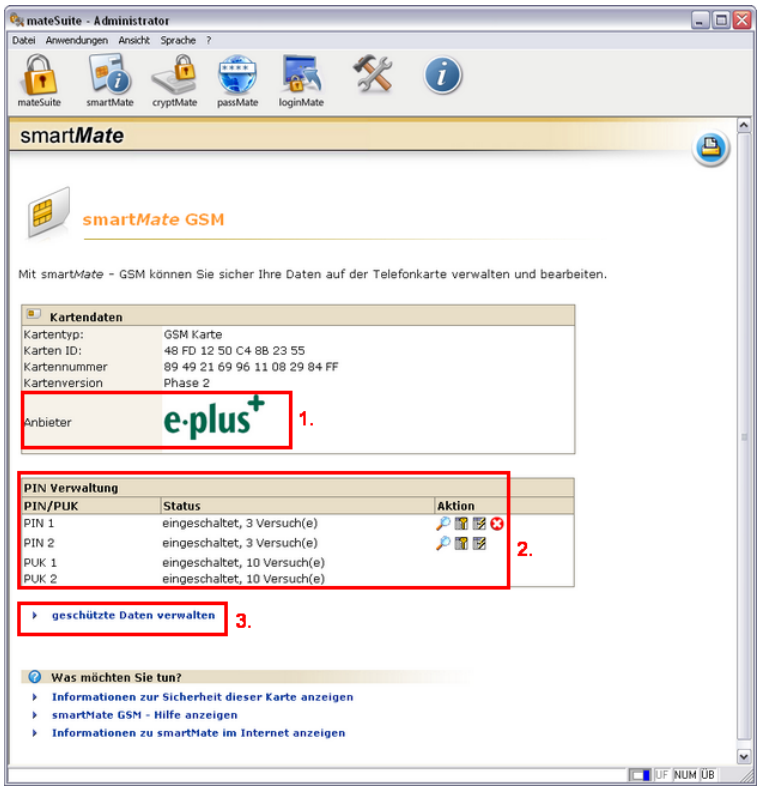
5.2.1.4.1 SmartCard Informationen einsehen

Um Informationen von SmartCards einzusehen, starten Sie den mateSuite-Administrator, wechseln Sie zu smart***Mate***® und führen Sie eine Karte in den Chipkartenleser ein. Die Daten werden ausgelesen und angezeigt.

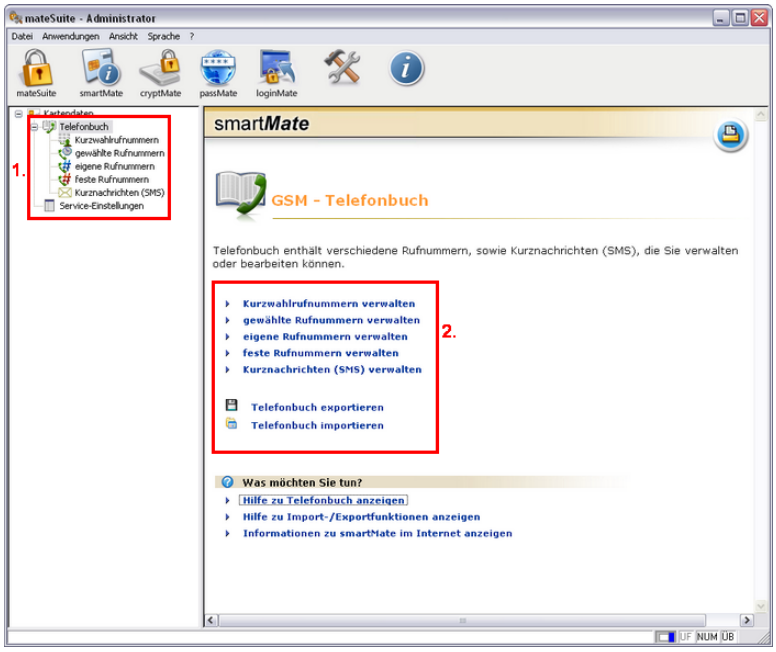
Sie können sich jetzt die angezeigten Informationen ausdrucken lassen, indem Sie Datei und Drucken klicken.

5.2.1.4.2 GSM Snap In

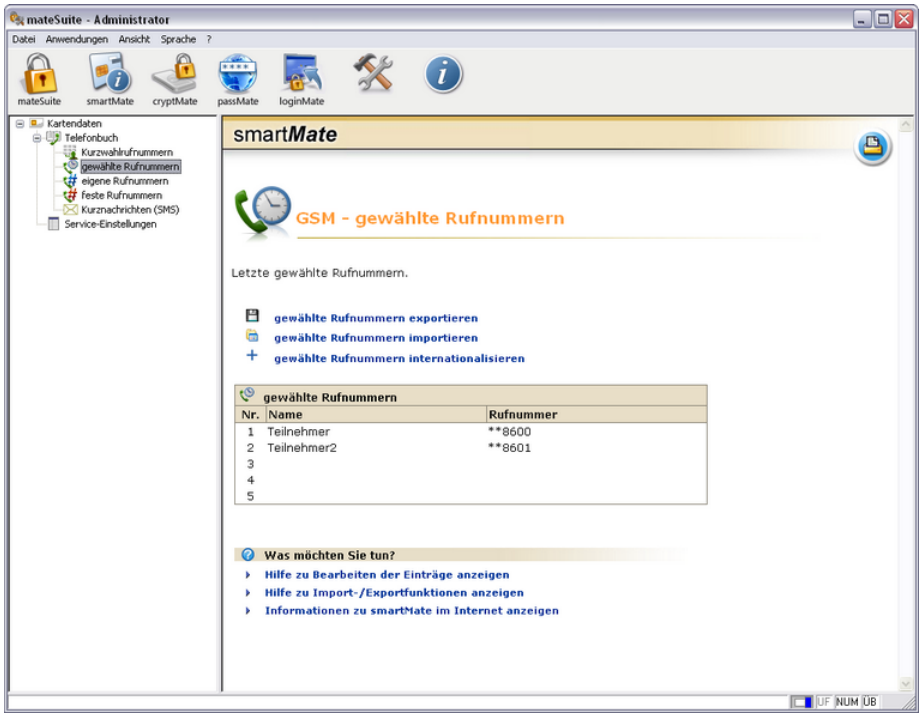
Für Telefonkarten, so genannten GSM Karten, bietet smart***Mate***® ein Snapin an, mit dem Sie bequem Ihre Daten auf der Telefonkarte verwalten und bearbeiten können. Das GSM-Snapin startet automatisch, wenn eine geeignete Karte eingeführt wird. Sie sehen Ihren Anbieter (1) und können bei der PIN Verwaltung (2) die PINs, die Sie von Ihrem Anbieter bekommen haben, ändern.



Drücken Sie *geschützte Daten verwalten* und Sie können die Daten auf Ihrer GSM-Karte bearbeiten.



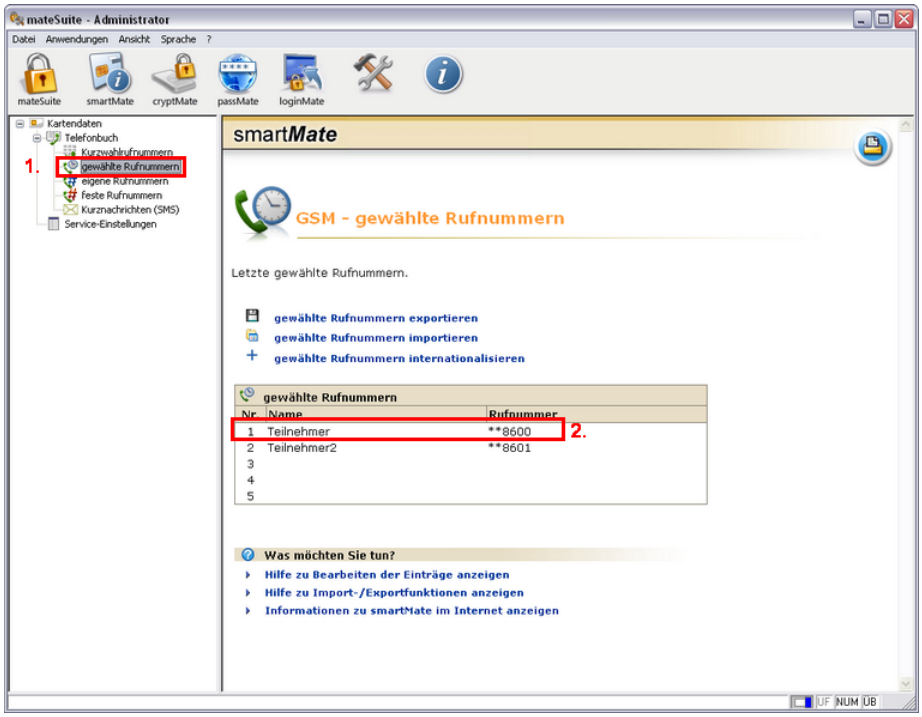
Das GSM-Snapin besteht aus einem zentralen Telefonbuch, das verschiedenen Telefonnummern und Kurznachrichten verwaltet. Sie können zwischen den einzelnen Nummern durch Anwahl der Schaltflächen auf der linken Seite des Dialogs (1) oder über die Menüeinträge unter (2) wechseln.



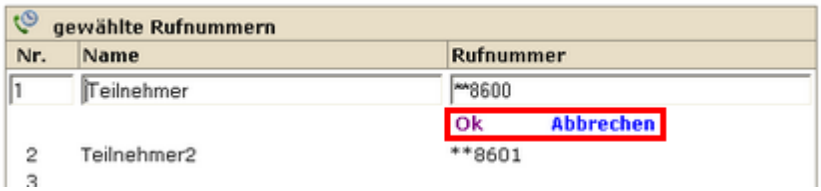
Beispiel: gewählte Rufnummern

5.2.1.4.2.1 Einträge bearbeiten/erstellen

Um Einträge zu bearbeiten, markieren Sie einen Eintrag im Telefonbuch. In unserem Beispiel verwenden wir die gewählten Rufnummern (1). Die Bearbeitung der anderen Nummern ist identisch.



Klicken Sie dann mit der linken Maustaste auf den zu ändernden Eintrag (2).



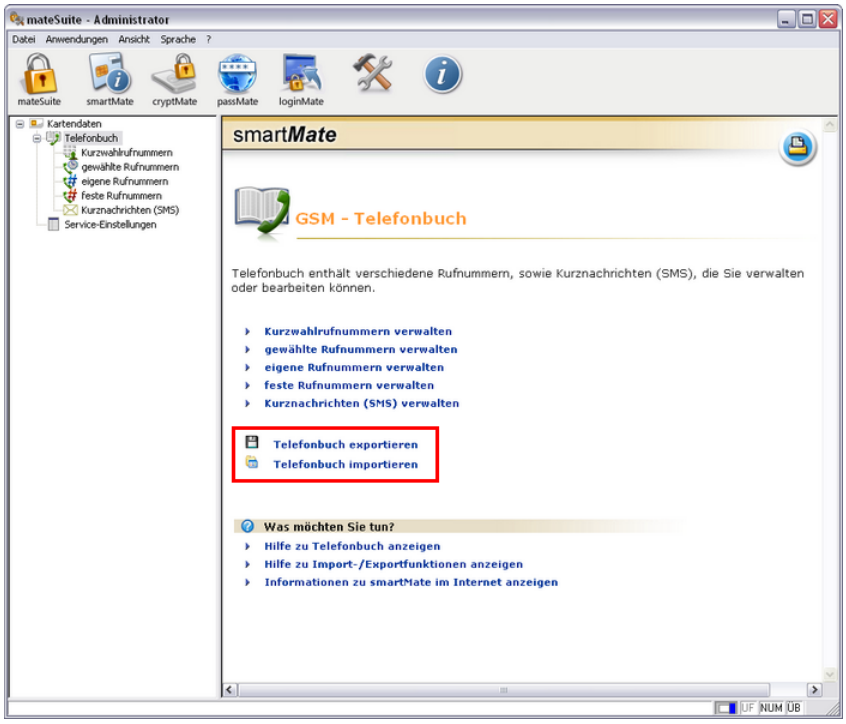
Sie können nun die laufende Nummer, den Namen und die Rufnummer ändern. Mit dem Button OK wird Ihre Änderung **sofort** auf Ihre Karte geschrieben.

Hinweis:

Sollten Sie die Nummer (Nr.) des Eintrags ändern, dann wird dieser Eintrag mit dem Eintrag der neuen Nummer getauscht.

5.2.1.4.2.2 Import/ Export

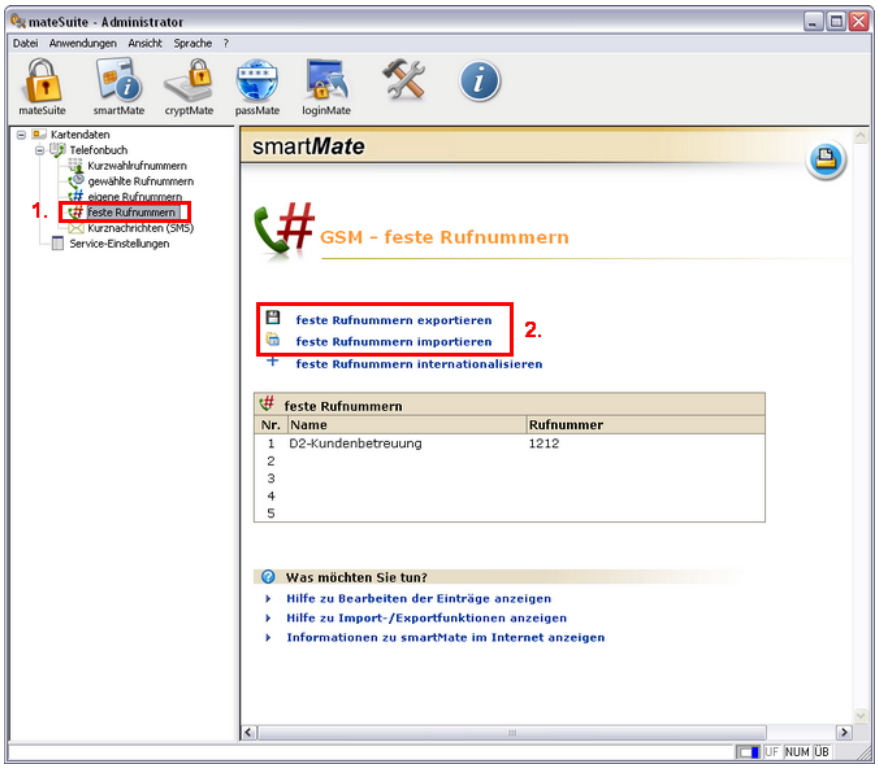
Sie können das gesamte Telefonbuch oder einzelne Komponente exportieren und wieder importieren.



Import/ Export des gesamten Telefonbuchs

Beim Export geben Sie einen Speicherort und den Namen der Datei an. Die exportierte Datei erhält die Dateiendung *.gsm.
Beim Import des gesamten Telefonbuches werden alle Daten auf der Karte überschrieben. Änderungen die seit dem letzten Export getätigt haben, gehen verloren.

Um eine einzelne Komponente des Telefonbuches zu exportieren oder zu importieren, wechseln Sie zu dieser Komponente in der linken Liste (1) und wählen die entsprechende Option (2) aus.

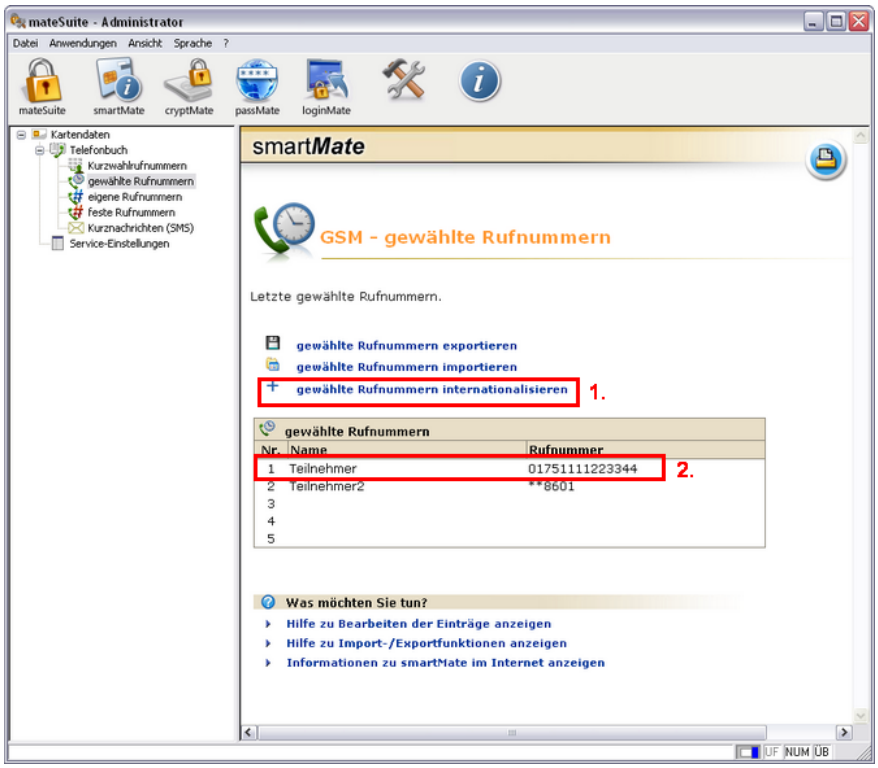


Beispiel: Export/ Import feste Rufnummern

Sie können auch einzelne Rufnummern, z.B. eigene Rufnummern, aus der Gesamtdatei des Telefonbuches importieren. Wählen Sie dazu beim Import die Gesamtsicherung (*.gsm) aus. Es wird nur diese Teilkomponente gelöscht und überschrieben,

5.2.1.4.2.3 Nummern internationalisieren

Sie haben mit dieser Funktion die Möglichkeit Nummern, die eine führende Null enthalten (2), zu internationalisieren (1). Diesen Nummern wird die entsprechende Landesvorwahl hinzugefügt.

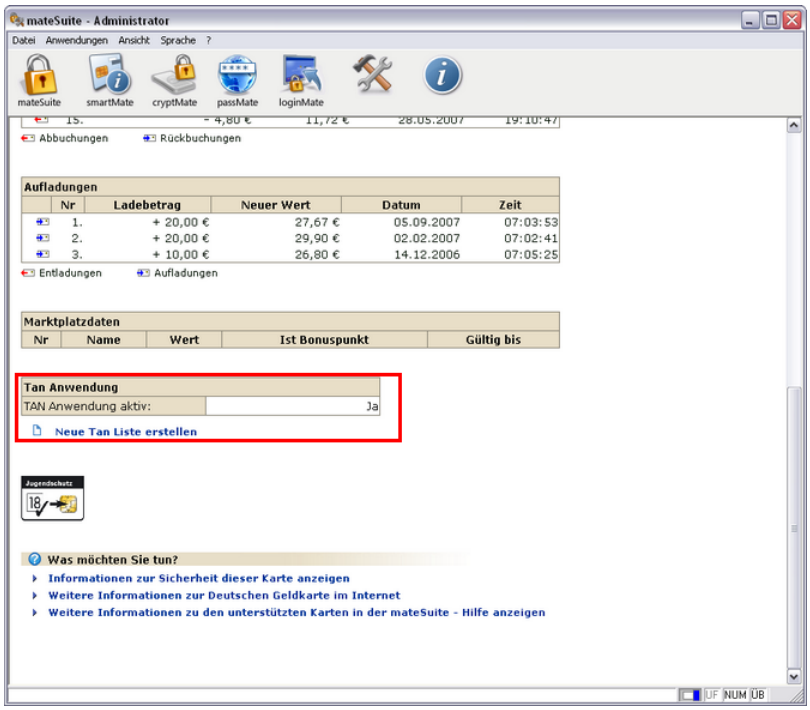


Wählen Sie Rufnummern internationalisieren (1) aus.

Welche Vorwahl sollen die Telefonnummern erhalten? Wählen Sie das entsprechende Land aus und alle Nummern mit führender Null werden internationalisiert.

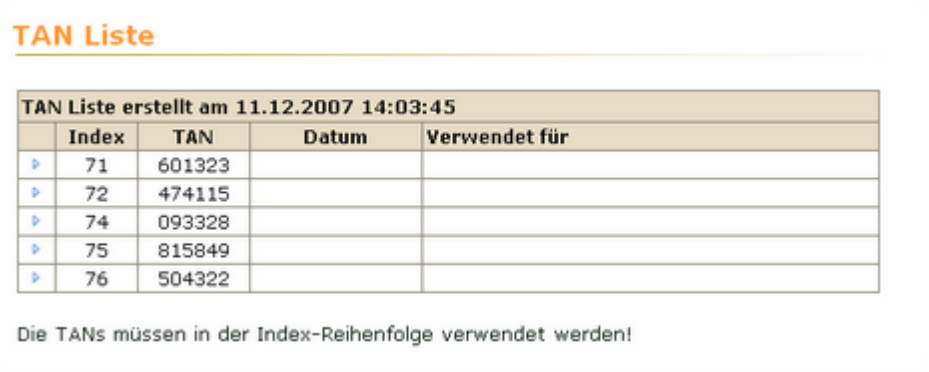
5.2.1.4.3 TAN-Generator

Bei deutschen EC-/Maestrokarten, die eine TAN-Anwendung haben, bietet smart***Mate***® die Möglichkeit zum Ausdruck von TAN-Bögen.



Ist eine Karte mit der TAN-Anwendung ausgestattet, wird dies in smartMate angezeigt. Durch Betätigen des Links *Neue TAN-Liste erstellen* gelangt man zum Auswahldialog zur Anzahl der zu erzeugenden TAN's.

Durch Betätigen des **Buttons OK** wird ein TAN-Bogen mit der gewünschten Anzahl TAN's generiert, der Platz zum Eintragen von Verwendungsdatum und -zweck lässt:



TAN Liste

TAN Liste erstellt am 11.12.2007 14:03:45				
	Index	TAN	Datum	Verwendet für
	71	601323		
	72	474115		
	74	093328		
	75	815849		
	76	504322		

Die TANs müssen in der Index-Reihenfolge verwendet werden!

Es ist darauf zu achten, dass die so erzeugten TAN's in der Indexreihenfolge verbraucht werden. Würde die Nummer 18 im Beispiel zuerst verwendet werden, so wären die Nummern 14-17 sofort ungültig.

Dieses moderne Verfahren wird noch nicht von allen Banken unterstützt. Im Zweifelsfall sollte vor Verwendung das jeweilige Kreditinstitut kontaktiert werden.

5.2.2 Verwaltung

Unter dem Menüpunkt **Anwendungen -> Verwaltung** können die zentralen Einstellungen zu mate ***Suite*** und dem Chipkartenleser vorgenommen werden.

mate***Suite*** fordert, für den korrekten Betrieb, den Zugriff auf den SmartCard Leser permanent. Damit andere Anwendungen (z.B. Homebankingprogramme) den Chipkartenleser verwenden können, ist es erforderlich, dass mateSuite die Kontrolle über den Chipkartenleser zeitweise abgibt.

Hierbei muss man zwei Arten von Anwendungen unterscheiden.
Anwendungen, die die **CTAPI-Schnittstelle** verwenden, werden von mateSuite beim Zugriff auf den Chipkartenleser automatisch erkannt und mateSuite startet einen Assistenten, um das weitere Vorgehen zu definieren. Hierbei können Sie den Zugriff für die Anwendung gewähren oder ablehnen. Gewähren Sie den Zugriff für diese Anwendung, so wechselt mateSuite in den Suspend Modus. In diesem Modus hat die Anwendung vollen Zugriff auf den Chipkartenleser und mateSuite befindet sich in einem Wartezustand. Beendet die Anwendung den Zugriff auf den Leser, so übernimmt mateSuite wieder die Kontrolle über den Chipkartenleser (Resume). mateSuite bietet Ihnen die Möglichkeit für alle Anwendungen ein vorgegebenes Verhalten zu definieren.

Anwendungen, die die **PC/SC-Schnittstelle** verwenden, werden beim Zugriff auf den Chipkartenleser nicht erkannt. Hierbei muss mateSuite von Ihnen manuell in den Suspendmodus gebracht werden. Hierbei hilft Ihnen der Suspend Manager.

Bitte informieren Sie sich im Handbuch Ihrer Anwendung, welche Schnittstelle Ihr Programm verwendet, um die entsprechenden Schritte auszuführen.

AutoSuspend-Anwendungen

Hier sind die AutoSuspend-Anwendungen aufgelistet, denen automatischer Zugriff auf den Chipkartenleser gewährt wurde. Die Anwendungen können hier wieder gelöscht werden.

mateSuite - Administrator
Datei Anwendungen Ansicht Sprache ?
mateSuite
smartMate
cryptMate
passMate
loginMate
Übersicht
AutoSuspend - Anwendu
Suspend - Manager
Bekannte Karten
Chipkartenleser
mateSuite Administrator
mateSuite AutoSuspend - Anwendungen
Damit andere Anwendungen (z.B. Homebankingprogramme) den Chipkartenleser verwenden können, ist es erforderlich, dass mateSuite die Kontrolle über den Chipkartenleser zeitweise abgibt. mateSuite - Autosuspend erkennt automatisch, dass eine andere Anwendung auf den Leser zugreifen möchte und fragt Sie, wie Sie weiter vorgehen möchten (AutoSuspend - Dialog). Hierbei können Sie den Zugriff für die Anwendung gewähren oder ablehnen. Gewähren Sie den Zugriff für diese Anwendung, so wechselt mateSuite in den Suspend Modus. In diesem Modus hat die Anwendung vollen Zugriff auf den Chipkartenleser und mateSuite befindet sich in einem Wartezustand. Beendet die Anwendung den Zugriff auf den Leser, so übernimmt mateSuite wieder die Kontrolle über den Chipkartenleser (Resume). mateSuite bietet Ihnen die Möglichkeit für alle Anwendungen ein vorgegebenes Verhalten zu definieren.
Sie können folgendes Standardverhalten festlegen:
Den Zugriff ohne Rückfrage immer zu gewähren
Den Zugriff ohne Rückfrage immer abzulehnen
Bei jedem Zugriff erneut zu fragen
Um ein vorgegebenes Verhalten zu definieren, wählen Sie einfach die Schaltfläche Optionen im AutoSuspend - Dialog (s.o). Alle Anwendungen, für die ein vorgegebenes Verhalten definiert ist, werden in folgender Tabelle aufgelistet.
AutoSuspend - Anwendungen
Nr
Anwendung
Pfad
Status
Aktion
*** Keine Anwendungen definiert ***
UF NUM ÜB

Suspend Manager-Einstellungen

Hier erfolgt die Einstellung, ob der Suspend Manager bei Systemstart automatisch geladen werden soll.

Bekannte Karten

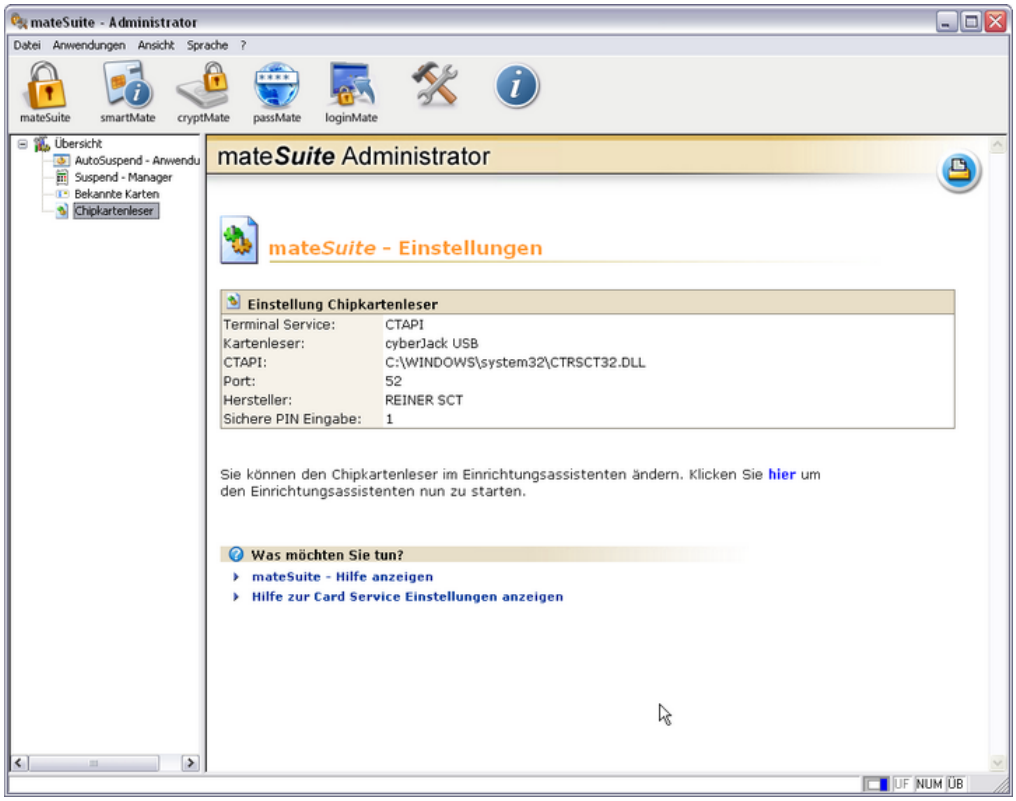
Hier können weitere Karten als Berechtigungen hinzugefügt werden.

Das Löschen von Bekannten Karten hat keinen Einfluss auf die einzelnen mate *Suite*-Objekte (passMate-Datenbanken, cryptMate-Laufwerke, loginMate-Konten).

Sollen die Rechte bestimmter Karten auf mate*Suite*-Objekte eingeschränkt werden, so müssen dafür die Berechtigungen für das einzelne mateSuite-Objekt geändert werden.

mate*Suite* Einstellungen

In den mate***Suite*** Einstellungen werden die Parameter für die Chipkartenleser-Schnittstelle angezeigt. Wenn Sie den Button **hier** klicken betätigen startet der Einrichtungsassistent und Sie können Änderungen an allen mate***Suite***-Anwendungen vornehmen.



Terminal Service	Momentan nur CTAPI
Kartenleser	Daten gemäß <hbcikrnl.ini>-Eintrag
CTAPI	dito
Port	dito
Hersteller	dito
Sichere PIN-Eingabe	dito

5.2.2.1 mateSuite Suspend Manager

Der Suspend Manager (engl.: to suspend = sperren) dient dazu, den Chipkartenleser unkompliziert für andere Anwendungen frei zu geben. Die Freigabe des Lesers wird notwendig, sobald Sie mit anderen Chipkarten-Applikationen als mate***Suite*** arbeiten wollen. Sie können den SmartCard Leser für jede Anwendung manuell freigeben, aber auch Anwendungen zum Suspend Manager hinzufügen (nur CTAPI-Anwendungen), um die Zugriffssteuerung auf den SmartCard Leser automatisch erfolgen zu lassen.

Durch die Voreinstellungen von mate***Suite*** wird der Suspend Manager automatisch beim Systemstart geladen. Im Infobereich der Taskleiste, können Sie den Suspend Manager starten.

Klicken Sie mit der rechten Maustaste auf das Chipkartenleser-Symbol:

Über das Menü können Sie die Funktionen des Suspend Managers nutzen. Es stehen folgenden Funktionen zur Verfügung:

Suspend

Damit kann der Zugriff von mate***Suite*** auf den Chipkartenleser durch linken Mausklick manuell abgeschaltet werden. In diesem Zustand können beliebige Anwendungen auf den Chipkartenleser zugreifen.

Wenn der Suspend Manager deaktiviert ist, erscheint folgendes Symbol:

Resume

Gibt den Zugriff des Chipkartenlesers für mate***Suite*** wieder frei, soweit dieser deaktiviert wurde.

Alternativ können Sie auch über Klick mit der linken Maustaste mateSuite sperren (Suspend) bzw. freigeben (Resume).

Arbeitsstation sperren

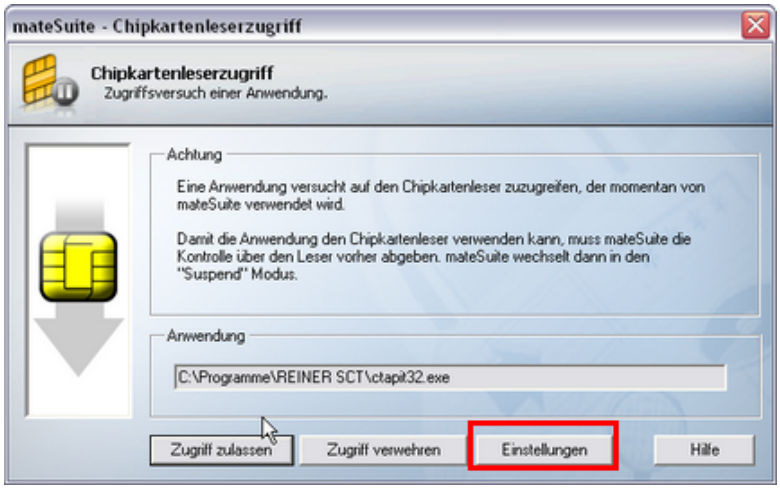
Sperrt die Arbeitsstation mittels login***Mate***.

Einstellungen

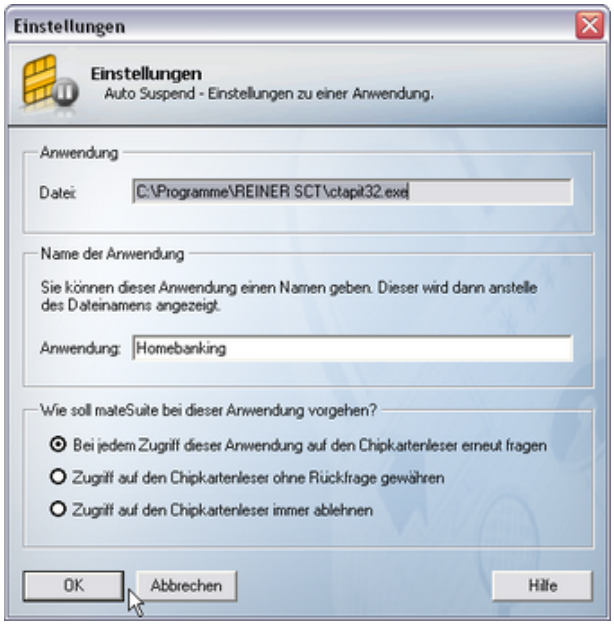
Startet mate***Suite*** unter Systemoptionen.

5.2.2.2 mateSuite AutoSuspend

mate***Suite*** AutoSuspend kontrolliert alle Zugriffe auf die CTAPI-Schnittstellen (Card Service) des Chipkartenlesers und erkennt automatisch, wenn eine andere Anwendung auf den Chipkartenleser zugreifen möchte. Damit ist die jederzeitige Kontrolle möglich, welche Anwendung wann auf das Gerät und die darin befindliche Karte zugreifen kann. AutoSuspend identifiziert dabei die Programmdatei, von der aus die Schnittstelle für den Chipkartenleser aufgerufen wird.


mateSuite - Chipkartenleserzugriff
Chipkartenleserzugriff
Zugriffsversuch einer Anwendung.
Achtung
Eine Anwendung versucht auf den Chipkartenleser zuzugreifen, der momentan von mateSuite verwendet wird.
Damit die Anwendung den Chipkartenleser verwenden kann, muss mateSuite die Kontrolle über den Leser vorher abgeben. mateSuite wechselt dann in den "Suspend" Modus.
Anwendung
C:\Programme\REINER SCT\ctapit32.exe
Zugriff zulassen
Zugriff verwehren
Einstellungen
Hilfe

Bei Anwendungen die häufig verwendet werden und die vertrauenswürdig sind, kann über die **Einstellungen** ein generelles Zugriffsrecht ohne Rückfragen gewährt werden. Anstelle der aufrufenden Programmdatei können Sie hier auch den Namen der Anwendung hinterlegen.



Wird der Chipkartenleser von einer anderen Anwendung verwendet als mate***Suite*** und Sie sperren manuell Ihren PC, dann können Sie entweder manuell Ihren Rechner wieder entsperren oder Sie entziehen der Anwendung den Zugriff auf den Chipkartenleser.

Der Hinweis **Card Service suspended** zeigt an, dass der Chipkartenleser nicht von mateSuite verwendet wird und somit zur Zeit nicht ansprechbar ist.
Klicken Sie auf **Informationen zum Fehler** und es öffnet folgendes Fenster.

mateSuite - loginMate
loginMate
Der Chipkartenleser ist gesperrt.
Status
Der Chipkartenleser wird momentan von einer anderen Anwendung verwendet.
Sie können die Arbeitsstation nun Entsperren/Herunterfahren, in dem Sie das Anmeldepasswort direkt eingeben (wählen Sie hierzu die Schaltfläche <manuell>) oder Sie entziehen der Anwendung die Kontrolle und stellen den Chipkartenleser mateSuite zur Verfügung.
Dies kann aber in der Anwendung, die momentan die Kontrolle über den Chipkartenleser hat, zu unvorhersehbaren Fehlern führen.
Anwendung
Anwendung: Homebanking
Prozess ID: 2692
Chipkartenleser mateSuite zuweisen
Abbrechen
Hilfe

Hier können Sie dem Chipkartenleser mate***Suite*** zuweisen und können sich dann mit der Chipkarte wieder anmelden.

Siehe auch

- mateSuite Administrator Verwaltung

5.2.2.3 Berechtigungen

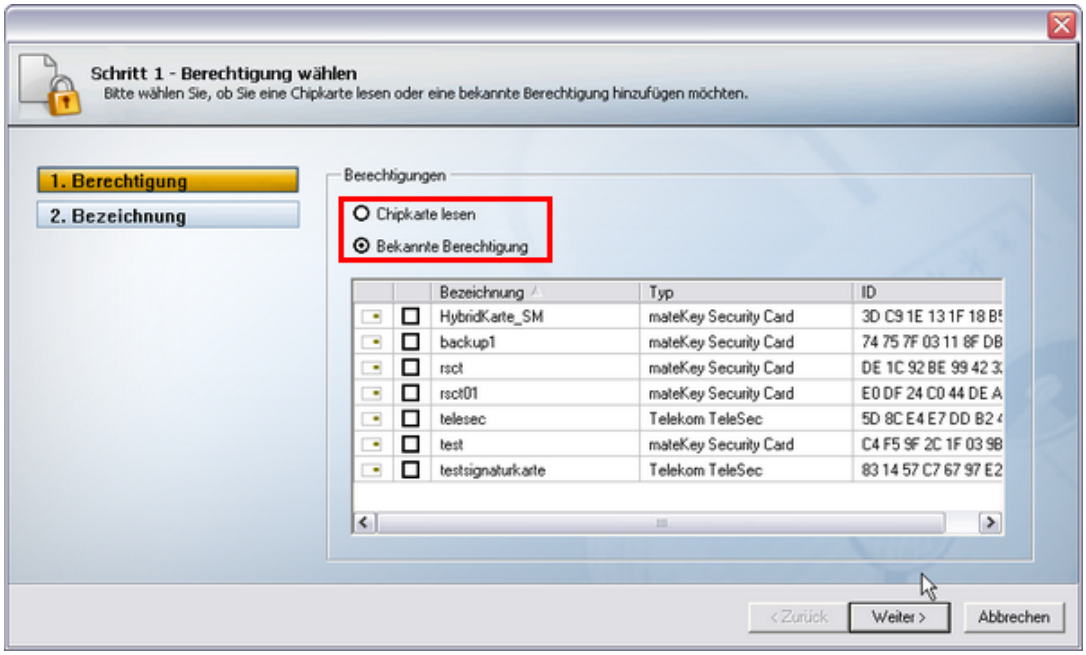
Für den Zugriff auf die verschiedenen mate***Suite***-Anwendungen werden Berechtigungen benötigt. Diese Berechtigungen sind im Grunde die erfassten Chipkarten. Der auf den Chipkarten enthaltene kryptografische Schlüssel wird verwendet, um die einzelnen Anwendungen zu verschlüsseln und zu sichern.

Die Chipkarten kann man entweder im Einrichtungsassistenten erfassen oder direkt im mateSuite-Administrator anlegen.

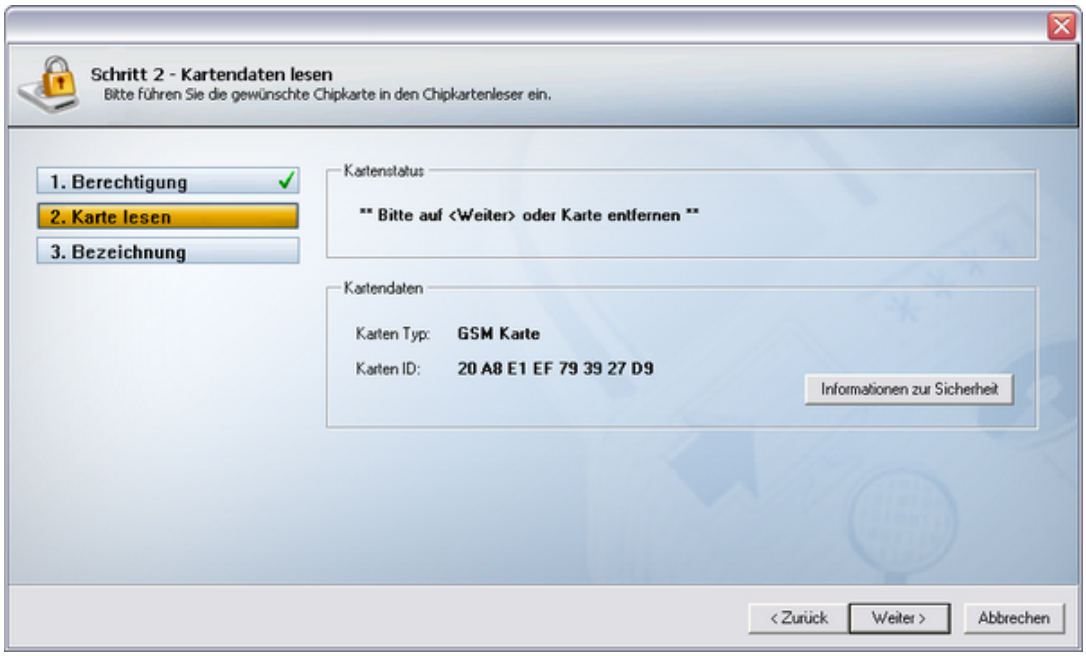
Berechtigungen einzelnen mateSuite Anwendungen hinzufügen

Das Hinzufügen von Berechtigungen läuft immer wie folgt ab.

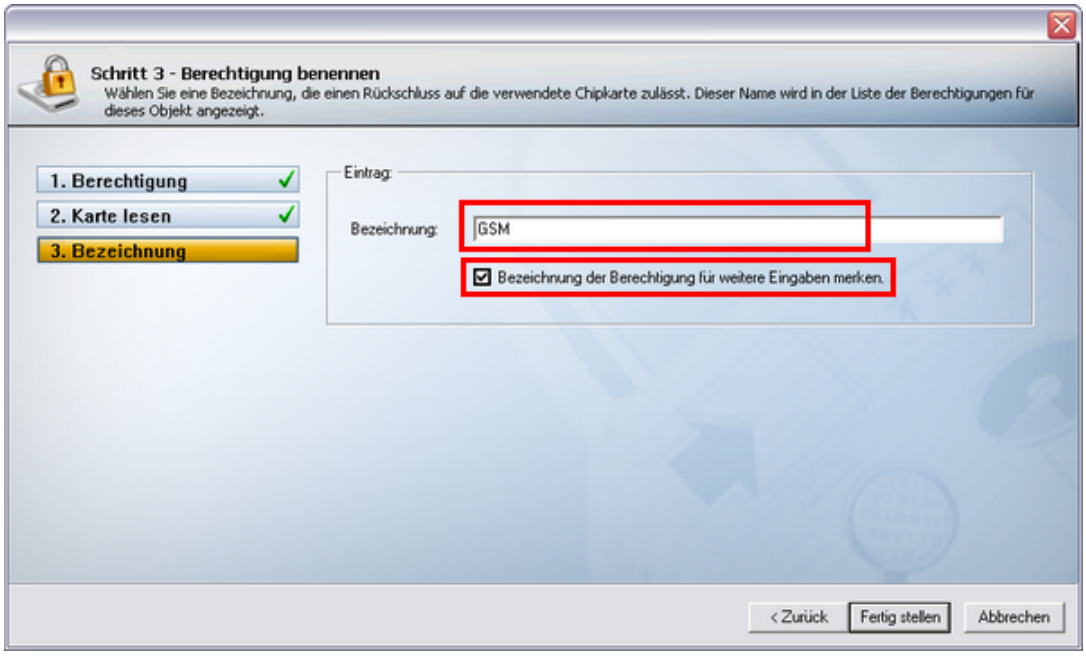
In diesem Schritt geben Sie die Berechtigungen an, die einen Zugriff auf die jeweilige Anwendungen erhalten sollen.
Klicken Sie auf den **Button Berechtigungen hinzufügen** und Sie können die Berechtigungen für die Anwendung definieren.



Sie können die Berechtigung aus bereits erfassten Karten (Bekannte Berechtigung) oder Sie können eine neue Chipkarte (Chipkarte lesen) als Berechtigung hinzufügen. Die bekannten Berechtigungen können Sie in der Tabelle auswählen. Mit dem **Button Weiter** übernehmen Sie die Berechtigung für diese Anwendung.
Bei **Chipkarte lesen** stecken Sie eine neue Karte in den Chipkartenleser und drücken ebenfalls **Weiter**. Folgen Sie dem Assistenten.


Schritt 2 - Kartendaten lesen
Bitte führen Sie die gewünschte Chipkarte in den Chipkartenleser ein.
1. Berechtigung
2. Karte lesen
3. Bezeichnung
Kartenstatus
** Bitte auf <Weiter> oder Karte entfernen **
Kartendaten
Karten Typ: GSM Karte
Karten ID: 20 A8 E1 EF 79 39 27 D9
Informationen zur Sicherheit
< Zurück
Weiter >
Abbrechen

Die neu eingeführte Karte wurde erkannt. Bestätigen Sie mit **Weiter**.


Schritt 3 - Berechtigung benennen
Wählen Sie eine Bezeichnung, die einen Rückschluss auf die verwendete Chipkarte zulässt. Dieser Name wird in der Liste der Berechtigungen für dieses Objekt angezeigt.
1. Berechtigung
2. Karte lesen
3. Bezeichnung
Eintrag:
Bezeichnung:
GSM
Bezeichnung der Berechtigung für weitere Eingaben merken.
< Zurück
Fertig stellen
Abbrechen

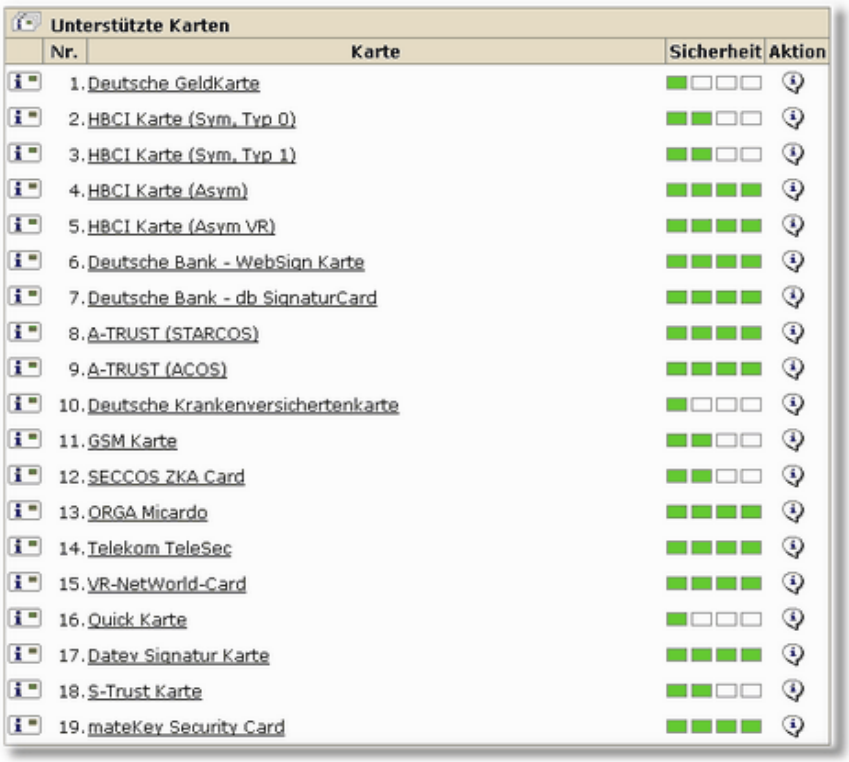
Geben Sie einen Namen für den Eintrag an.
Durch Aktivierung der Option *Merke den Schlüsselnamen für weitere Eingaben* wird bei späterem Einstecken der Karte immer genau der vorgegebene Name angezeigt.

Klicken Sie auf Weiter und die eingerichteten Chipkarten/Berechtigungen werden nun angezeigt.

Bei PIN-geschützten Chipkarten ist an dieser Stelle die Eingabe der PIN erforderlich!

6 Unterstützte Chipkarten

mate***Suite*** unterstützt folgende Chipkarten:



Unterstützte Karten

Nr.	Karte	Sicherheit	Aktion
1.	Deutsche GeldKarte		
2.	HBCI Karte (Sym. Typ 0)		
3.	HBCI Karte (Sym. Typ 1)		
4.	HBCI Karte (Asym)		
5.	HBCI Karte (Asym VR)		
6.	Deutsche Bank - WebSign Karte		
7.	Deutsche Bank - db SignaturCard		
8.	A-TRUST (STARCOS)		
9.	A-TRUST (ACOS)		
10.	Deutsche Krankenversichertenkarte		
11.	GSM Karte		
12.	SECCOS ZKA Card		
13.	ORGA Micardo		
14.	Telekom TeleSec		
15.	VR-NetWorld-Card		
16.	Quick Karte		
17.	Datev Signatur Karte		
18.	S-Trust Karte		
19.	mateKey Security Card		

Diese unterschieden sich in Ihrer Sicherheit vor allem in den Punkten PIN-Unterstützung und Schlüssellänge. Über die grüne Sicherheitsanzeige lässt sich ein Grad der Sicherheit erkennen und somit grafisch verdeutlichen.

6.1 mateKey Security Card

Die mate***Key*** Security Card ist eine RSA-Kryptokarte und wird auch als solche von vielen Kreditinstituten in Sicherheitsanwendungen eingesetzt. Sie bietet 32 KB Speicherplatz zum Speichern von pass***Mate***®-Einträgen und login***Mate***®-Konten.

Im Gegensatz zur Datenbank-Speicherung ist die mate***Key***-Karte mobil einsetzbar, so dass man mit einer Karte, seine Passwörter jederzeit aktuell zu Hause und im Büro auf verschiedenen Rechnern parat hat.

Initiale PIN

Die initiale PIN (Personal Identification Number) der mate***Key*** Security Card dient der Absicherung der auf der Karte gespeicherten Daten. Die Karte verfügt über einen sogenannten

Fehlbedienungszähler. Wird die PIN acht Mal falsch eingegeben, so wird die Karte gesperrt und kann nur noch mit der PUK (Master PIN) freigeschaltet werden. Die PIN hat im Auslieferungszustand den Wert **00000.**

PUK

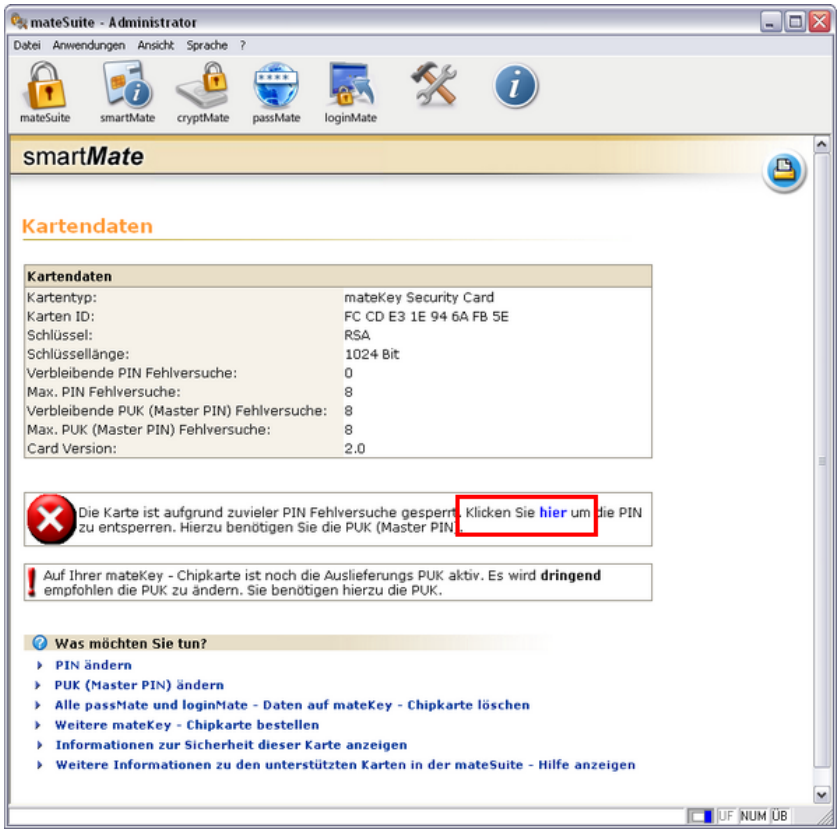
Die Karte ist mit einer PUK (Personal Unblock Key) ausgestattet. Die PUK dient dazu, an einem sicheren Ort hinterlegt zu werden, um bei einer eventuellen PIN-Sperre durch zu häufige Falscheingaben, diese wieder freischalten zu können. Um die Sicherheit zu erhöhen, ist es zu empfehlen die PUK zu ändern. Wird die PUK acht Mal falsch eingegeben, so ist die Karte endgültig gesperrt. Die PUK hat im Auslieferungszustand den Wert **00000000.**

Folgende Sicherheitshinweise sollten unbedingt beachtet werden:

- Vor dem Speichern von Daten auf der mate***Key***-Karte sollte die PIN auf alle Fälle geändert werden.
- PIN und PUK sollten auf keinen Fall auf die Karte geschrieben oder auf sonst eine Weise Dritten zugänglich gemacht werden.

Entsperren der mate*Key* Security Card

Wenn Sie acht Mal die PIN falsch eingegeben haben, wird die Karte gesperrt. Um die Karte zu entsperren benötigen Sie den PUK.
Wechseln Sie hierfür in das smart***Mate***® Modul. Sie erhalten den Hinweis das Ihre Karte aufgrund zu vieler PIN Fehlversuche gesperrt wurde.


mateSuite - Administrator
Datei Anwendungen Ansicht Sprache ?
mateSuite
smartMate
cryptMate
passMate
loginMate
smartMate
Kartendaten
Kartendaten
Kartentyp: mateKey Security Card
Karten ID: FC CD E3 1E 94 6A FB 5E
Schlüssel: RSA
Schlüssellänge: 1024 Bit
Verbleibende PIN Fehlversuche: 0
Max. PIN Fehlversuche: 8
Verbleibende PUK (Master PIN) Fehlversuche: 8
Max. PUK (Master PIN) Fehlversuche: 8
Card Version: 2.0
Die Karte ist aufgrund zuvieler PIN Fehlversuche gesperrt. Klicken Sie hier um die PIN zu entsperren. Hierzu benötigen Sie die PUK (Master PIN).
Auf Ihrer mateKey - Chipkarte ist noch die Auslieferungs PUK aktiv. Es wird dringend empfohlen die PUK zu ändern. Sie benötigen hierzu die PUK.
Was möchten Sie tun?
PIN ändern
PUK (Master PIN) ändern
Alle passMate und loginMate - Daten auf mateKey - Chipkarte löschen
Weitere mateKey - Chipkarte bestellen
Informationen zur Sicherheit dieser Karte anzeigen
Weitere Informationen zu den unterstützten Karten in der mateSuite - Hilfe anzeigen
UF NUM ÜB

Klicken Sie auf **hier** und folgen Sie den Anweisungen.

Beachten Sie Bitte bei der Entsperrung:

- Sie werden bei der Entsperrung aufgefordert eine Geheimzahl einzugeben, **bitte geben Sie hier Ihren PUK ein**.
- Dann geben Sie Ihre neu gewählte PIN zweimal ein und bestätigen jeweils mit OK.

7 Unterstützte Chipkartenleser

mate***Suite*** unterstützt alle Chipkartenleser, die folgenden technischen Anforderungen genügen:

- Unterstützung der CTAPI-Schnittstelle
- ISO 7816, Teil 1-4
- EMV 2.0

mate***Suite*** findet dabei alle Chipkartenleser, die sich in die Datei <hbcikrnl.ini> im Windows-Systemverzeichnis eintragen. Ist dies nicht der Fall, so muss der Pfad zur richtigen DLL-Datei manuell in den Einstellungen des mate***Suite*** Cardservice eingetragen werden.

Die Unterstützung der PC/SC-Schnittstelle wird nach erfolgter Freigabe der PC/SC-Spezifikation 2.0 zu einem späteren Zeitpunkt implementiert.

8 Anregungen/Support/Updates

Es ist uns wichtig, dass Sie mit unserem Produkt zufrieden sind. Bei Fragen, Anregungen und für technische Unterstützung stehen wir Ihnen unter den folgenden Kontaktadressen gerne zur Verfügung:

Fragen, Anregungen

Fehlt Ihnen ein Feature? Möchten Sie uns von einem Fehler berichten? Dann kontaktieren Sie uns per E-Mail unter der Adresse mateSuite@reiner-sct.com.

Support, FAQs

Bei technischen Fragen und Problemen steht Ihnen unser Support unter support@reiner-sct.com gerne zur Verfügung.

Antworten auf die häufigsten Fragen zur mateSuite finden Sie auch in unseren FAQs.

Updates

Im mate***Suite***-Administrator unter **? | Updates** können Sie jederzeit überprüfen, ob eine neuere Version verfügbar ist.

Falls Sie mate***Suite*** mit einem Chipkartenleser aus unserer cyberJack-Familie betreiben, können Sie mate***Suite*** auch über die Funktion Aktualisierung im cyberJack-Gerätemanager unter **Start | Programme | REINER SCT cyberJack | Gerätemanager, Funktionstest** auf den neuesten Stand bringen.

9 mateSuite-Glossar

Asymmetrische Verschlüsselung (RSA)

Mit dieser Verschlüsselungsart wird die Digitale Signatur erzeugt, die dann sicher versandt und gelesen werden kann. Dabei existiert ein Schlüsselpaar aus einem "öffentlichen", frei zugänglichen und dem "privaten" Schlüssel des Benutzers. Diese Schlüssel werden von Zertifizierungsstellen oder "Trust Centers" verwaltet. Dort kann sich ein Internet-User persönlich registrieren lassen, erhält dann seine Chipkarte mit dem privaten Schlüssel und kann diesen z.B. für Homebanking mit HBCI nutzen.

crypt*Mate*®-Laufwerksdatei

Beim Einrichten eines virtuellen Laufwerks muss eine crypt***Mate***® Control-Datei erstellt werden. Auf Basis dieser Datei wird das virtuelle Laufwerk erstellt. Die Datei stellt das virtuelle Laufwerk in verschlüsselter Form dar. Daher muss die crypt***Mate***® Control-Datei beim Aktivieren eines virtuellen Laufwerks von crypt*Mate* gelesen werden und einem Schlüssel zugeordnet werden.

SmartCard

Die Begriffe Chipkarten und SmartCards werden synonym verwendet.

pass*Mate*®-Datenbank

In einer pass***Mate***® Datenbank werden die Anmeldedaten für eine Anwendung oder Website gespeichert. Die Datenbanken können nur in Verbindung mit der zugeordneten SmartCard gelesen werden. Somit ist maximale Datensicherheit gewährleistet.

Index

- A -

Administrator 3, 5, 20, 21
Anregungen 78
Anwerndungen 67
AutoSuspend 71

- B -

Berechtigungen 7, 68, 73

- C -

Chipkarten 7, 73, 76
Chipkartenleser 6
cryptMate 16, 48
cryptMate-Manager 54
Datei/ Ordner verschlüsseln 57
Dateien verschlüsseln und entschlüsseln 56
Einstellungen 55
Sicher löschen 59
Verschlüsseln 49
virtuelle Laufwerke bearbeiten 51
virtuelle Laufwerke verwalten 51
virtuelles Laufwerk erstellen 49
CT-API 78

- D -

Datenbank 12

- E -

Einführung 3
Einrichtung 6, 9, 12, 16
Einrichtungsassistent 5
Entsperren 76
Erfassen 7
Erweiterte Anmeldung 27

- F -

Fremdanwendungen 67

- G -

GSM Snapin
Eintrage bearbeiten, löschen, ändern 62
GSM-Snapin
Import/ Export 63
Nummern internationalisieren 65

- K -

Kontenbeschränkung 27

- L -

Lizenzinformationen 4
loginMate 9, 22
Anmeldung manuell 29
Anmeldung mit Chipkarte 29
Beenden 34
Benutzerkonto wählen 31
Berechtigung hinzufügen 11
Einstellungen 36
Funktion STRG+ALT+ENTF 34
Kontenverwaltung 25
Konto erstellen 10, 23
Runterfahren manuell 34
Runterfahren mit Chipkarte 34
Sperren manuell 31
Sperren mit Chipkarte 31

- M -

mateKey 76
mateSuite 20, 21

- O -

öffentlicher Schlüssel 68

- P -

passMate 12, 37
Einstellungen 47
Passworteinträge 38
Passworteinträge bearbeiten 41
Plugin Internet Explorer 42
passMate-Manager 45
PC/SC 78
PIN 76
PUK 76

- S -

Security Card 76
smartMate 60

smartMate 60
GSM Snapin 61
SmartCard Informationen 60
Tan-Generator 66
Telefonkarte 61
Support 78
Suspend 67
Suspend Manager 70
Systemvorbereitung 6

- U -

Updates 78

- V -

Version 4
Verwaltung
Administrator 67
Bekannte Karten 67
mateSuite 67

- Z -

Zielfenster 40

REINER Kartengeräte GmbH & Co. KG

Goethestrasse 14
78120 Furtwangen
Germany

Telefon: +49 (0)7723-5056-0
Telefax: +49 (0)7723-5056-78
E-Mail: mail@reiner-sct.com
Internet: www.reiner-sct.com